Product Manual
PCU-200 Series with Firmware Version 1.28.0

DILAX Intelcom GmbH
Alt-Moabit 96b
10559 Berlin

www.dilax.com
info@dilax.com

Author: SMA, AVO, WKL, FHA
Version: 1.0
Date: 13.07.2017

Version history

Version	Change	Author	Reviewer	Publisher	Valid from
1.0	Supplement to controlling the recording of passenger information data for recording in CSV format in Chapter 3.16.1 On receiving PIS data and position data when configuring vehicle signals via the remote information services. Note in Chapter 3.21.3 changed so that the PCU must be restarted when any change is made to the configuration. Note in Chapter 3.11.3 added. Permanent GPRS connection for securely setting the system time with SNTP. Chapter 4.1 rewordings.	AVO	HRA, KME	AGO	07.07.2017

Contents

1 Introduction PCU-200 series 15
1.1 Architecture 15
1.2 Models 16
1.3 Key features 21
2 Hardware Installation 22
2.1 Mechanical Mounting Instructions 22
2.2 Power Consumption in Standby Mode 22
2.3 Grounding concept 22
2.4 Connectivity and Signal Description 23
2.4.1 PCU-200 Models without LEDs for digital inputs/outputs (G1) 23
2.4.2 PCU-200 Models with LEDs for digital inputs/outputs (G2) 24
2.4.3 Main Connectors X01 and X02 (Power Supply, DILAX LAN, Digital Inputs) 25
2.4.3.1 Digital Inputs IN1-IN4 28
2.4.3.2 IN5 (Odometer Input for Driving Speed Calculation) 29
2.4.3.3 Wiring examples 30
2.4.4 Serial Sensor Link SSL (X03) 31
2.4.5 Ethernet ETH (X04, X06) 32
2.4.5.1 M12 Ethernet connector 33
2.4.5.2 RJ45 Ethernet connector 33
2.4.6 GSM/WLAN Antenna Connector (X07) 33
2.4.7 GPS Antenna Connector (X08) 33
2.4.8 SIM Card Slot (X09) 34
2.4.9 Rear Connectors X10 and X11 (Digital Outputs, Digital Inputs, Odometer) 34
2.4.9.1 IBIS-VDV300 Interface 36
2.4.9.2 Digital Outputs 37
2.4.9.3 Digital Inputs 6 and 7 38
2.4.9.4 Digital Input 8 39
2.4.9.5 Wiring examples 40
2.4.10 Connector for accessory modules (X12, option) 40
2.4.11 Status indicators (LEDs) 41
2.5 Accessories 42
2.5.1 Configuration Plug SST-100 (X12, Option) 42
2.5.1.1 Dimensioned drawings SST-100 43

2.5.1.2 Mounting SST-100 43
2.5.1.3 Technical Data SST-100 44
2.5.1.4 Trouble shooting SST-100 44
2.5.1.5 Ordering Information SST-100 44
2.5.2 Pull-down Resistor PDR-100 45
2.5.2.1 Connection wiring and block diagram PDR-100 46
2.5.2.2 Mounting PDR-100 46
2.5.2.3 Dimensioned Drawings PDR-100 47
2.5.2.4 Technical Data PDR-100 47
2.5.2.5 Ordering Information PDR-100 48
3 Configuration 49
3.1 Opening the Web Interface 49
3.2 Overview of the Operating Elements 50
3.3 Password Protected Accessing the Web Interface 51
3.4 Saving the Configuration 52
3.5 Configuration > System > General 52
3.6 Configuration > Communication > Network 57
3.6.1 Automatic IP configuration (DHCP) 57
3.6.2 Manual IP configuration 58
3.7 Configuration > System > Doors 59
3.8 Configuration > System > Rooms 65
3.9 Configuration > System > Vehicle Signals 71
3.10 Configuration > Positioning Data 75
3.10.1 Choosing a Positioning Data Source 77
3.10.2 Recording of Raw Position Data 77
3.11 Configuration > Communication > GSM 77
3.11.1 Defining Provider Settings 78
3.11.2 Defining Data Connection Settings 79
3.11.3 Defining Network Settings 80
3.11.4 Defining GSM Security Settings 81
3.11.5 Defining Dial-In Settings 81
3.12 Configuration > Communication > FTP Server Configuration 82
3.13 Configuration > Communication > FTP Client Configuration 83
3.14 Configuration > Communication > SMTP 85
3.15 Configuration > Communication > HTTP Client 86

3.15.1 Secure data connection via HTTPS (data encryption) 89
3.16 Configuration > Recording & Output > Data Recording 93
3.16.1 PCU usage in mobile applications (vehicles) 94
3.16.2 PCU usage in stationary applications (buildings) 100
3.17 Configuration > Recording & Output > Live Tracking 100
3.18 Configuration > Recording & Output > Live Diagnostics 103
3.19 Configuration > System > Clients 104
3.19.1 Common Description of the Configuration of Clients 105
3.19.2 DCP Level 1 Client Configuration 107
3.19.3 Using the Remote Information Provider Function 109
3.19.3.1 Remote Information Provider > Installation Helpers 110
3.19.3.2 Synchronizing the System Time of the Master PCU with the System Time of the Client PCU 110
3.19.3.3 Receiving Diagnostic Data from the Client PCU 111
3.19.3.4 Remote Information Provider > Vehicle Signals 112
3.19.3.5 Remote Information Provider > Positioning Data 114
3.19.3.6 Remote Information Provider > Comm. Protocols 116
3.19.3.6.1 IBIS (VDV300) Protocol 116
3.19.3.7 Remote Information Provider > Digital Outputs 118
3.20 Configuration > Communication > Wi-Fi 119
3.21 Configuration > Communication > Comm. Protocols 122
3.21.1 J1708/J1587 Protocol 122
3.21.2 IBIS (VDV300) Protocol 122
3.21.3 IBIS (VDV300) Door Client 124
3.21.4 DCP Level 1 Protocol 126
3.22 Configuration > Recording & Output > Digital Outputs (PCU-220 and PCU-250) 127
4 Maintenance 130
4.1 Clock Synchronization 130
4.2 Loading / Saving the Configuration from or to a File 130
4.2.1 Saving the Device Configuration to a File 130
4.2.2 Loading the Device Configuration from a File 131
4.2.3 Validate hardware configuration 132
4.2.4 Extended Configuration Options for Loading the Device Configuration from a File 132
4.3 Usage of the Configuration Plug 134
4.3.1 Permanent Mode 135

4.3.2 Auto Mode 136
4.3.3 Requesting the State of the Configuration Plug 137
4.4 Firmware Update 137
4.4.1 Firmware Update via Web Interface 138
4.4.2 Automatic Firmware Update via FTP 139
4.5 Remote Access via GSM Dial-In 140
5 Troubleshooting 142
5.1 Logging, Error Handling and Watchdog 142
5.2 Creating an error report 144
5.3 Unlock Web Interface When Password is Lost 145
5.4 Testing Sensor Setup 145
5.4.1 Device State > Live Counting View 146
5.4.2 Device State > Device Information 146
5.5 Diagnostic Messages 148
5.6 Maintaining Client PCUs 152
5.7 Testing GSM/GPRS Communication 154
5.8 Scan for available Wi-Fi Network Stations 155
5.9 Testing Wi-Fi Communication 155
5.10 Testing FTP Client Configuration 156
5.11 Testing SMTP Configuration 157
5.12 Testing HTTP Client Configuration 157
5.13 Testing IBIS Communication 158
5.14 Checking the odometer pulses calibration 158
5.15 Trouble Shooting Guide 160
5.16 Resolving Ethernet Problems 162
5.17 Expert Mode 164
5.18 Resolving Configuration Saving Problems 164
5.19 Check current Hardware Configuration at Firmware Update 165
6 Appendix 166
6.1 Technical Data PCU-200 166
6.1.1 Electrical Data 166
6.1.2 Mechanical Data 166
6.1.3 Environmental Data 166
6.2 Counting Data Protocols 166
6.2.1 Data Transmission over FTP 167

6.2.2 DILAX Counting Protocol (DCP) 167
6.2.3 J1587 (J1708) 167
6.3 Timing Characteristics 167
6.4 Drawings 168
6.5 Block Diagram 170
7 Glossary of Acronyms and Abbreviations 171

List of figures

Figure 1: Master/client configuration of mobile systems 15
Figure 2: IP40 surface-mounted housing (metal shell) 16
Figure 3: IP54 surface-mounted housing 16
Figure 4: IP40 rack housing 16
Figure 5: Minimum distances to be considered for installation 22
Figure 6: IP40 housing grounding stud location 23
Figure 7: IP54 housing grounding stud location 23
Figure 8: Connectivity of PCU-200 models without LEDs for digital inputs/outputs at the front (G1) 24
Figure 9: Connectivity of PCU-200 models with LEDs for digital inputs/outputs at the front (G2) 25
Figure 10: Main connector 26
Figure 11: Principle of digital input circuit 1-4 28
Figure 12: Principle of digital input circuit IN5 29
Figure 13: Digital inputs with external contacts (door contacts) 30
Figure 14: DC switched isolated digital inputs (function ignition active and use of the 5th digital input with reference potential GND) 30
Figure 15: DC switched isolated digital inputs (without ignition) 31
Figure 16: Example for an invalid wiring 31
Figure 17: Digital inputs with different voltages 31
Figure 18: SSL connector 32
Figure 19: Ethernet connector M12 33
Figure 20: Ethernet connector RJ45 33
Figure 21: Rear connectors X10 and X11 35
Figure 22: Principle of digital output circuit 1-4 37
Figure 23: Principle of digital input 6 38
Figure 24: Principle of digital input 7 38
Figure 25: Principle of digital input 8 39
Figure 26: Digital outputs and digital inputs 6, 7 and 8 40
Figure 27: Digital outputs 40
Figure 28: SST-100 configuration plug 42
Figure 29: SST-100 connector 42
Figure 30: Dimensions SST-100 43
Figure 31: SST-100 mounting 43
Figure 32: Pull-down resistor PDR-100 45
Figure 33: PDR-100 connector 45

Figure 34: Connection wiring (left) and block diagram (right) PDR-100 46
Figure 35: Mounting PDR-100 46
Figure 36: Dimensions PDR-100 47
Figure 37: Web interface (example view) 49
Figure 38: Configuring a password to protect the web interface usage 51
Figure 39: Authentication dialog box 51
Figure 40: Load / Save page 52
Figure 41: Reboot the device 52
Figure 42: Configuration of general device settings 52
Figure 43: Master/client configuration of mobile systems 54
Figure 44: Configuration of the Ethernet network interface 57
Figure 45: Manual IP configuration of the Ethernet network interface 58
Figure 46: Configuration of the doors 59
Figure 47: Configuration of the door contacts 61
Figure 48: Configuration of the sensor bar 61
Figure 49: First sensor left 62
Figure 50: First sensor right 62
Figure 51: Examples for maximum coverage 63
Figure 52: Configuration of a sensor of a sensor bar 64
Figure 53: Configuration of the sensor blind-out input 64
Figure 54: Examples for correct room definitions 66
Figure 55: Examples for wrong room definitions 67
Figure 56: Names for inner and outer side of doors when having two rooms, an interior door and two outer doors 69
Figure 57: Configuration of rooms 69
Figure 58: Configuration of common input types 71
Figure 59: Configuration of the odometer input 72
Figure 60: Configuration of an event generation 73
Figure 61: Configuration of the positioning data settings 75
Figure 62: Configuring the settings for position determination for an external GPS receiver. 75
Figure 63: Configuration of the GSM/GPRS communication 78
Figure 64: Defining GSM/GPRS network settings 80
Figure 65: Defining GSM/GPRS security settings 81
Figure 66: Configuration of the build-in FTP server 83
Figure 67: Configuration of the build-in FTP client 84
Figure 68: Configuration of the SMTP client 86

Figure 69: Configuration of the HTTP client 87
Figure 70: Definition of certificates during configuration of the HTTP client 89
Figure 71: Example of a Server Certificate File in PEM format containing the X.509 certificate of a CA 91
Figure 72: Example of a Client Certificate File in PEM format containing the private RSA key and the X.509 certificate of the client 92
Figure 73: Example of a client certificate file in PEM format with password, private RSA key and X.509 client certificate 93
Figure 74: Configuration of DLX3 data recording for a mobile system 94
Figure 75: Configuration of CSV data recording for a mobile system 94
Figure 76: Display of the current CSV recording file 99
Figure 77: Configuration of data recording for a stationary system 100
Figure 78: Configuration of live tracking 101
Figure 79: Configuration of Live diagnostics 103
Figure 80: Configuration of the client PCUs managed by a master device 105
Figure 81: Configuration of client PCU detection for a variable train assembly 107
Figure 82: Client configuration with a DCP Level 1 network 108
Figure 83: Master PCU using master functionality provided by client PCUs 109
Figure 84: Remote information provider 109
Figure 85: Installation helpers for remote information provider 110
Figure 86: Only one client PCU may be used for time synchronization 110
Figure 87: Time synchronization via remote information provider 111
Figure 88: Receiving vehicle signals via client PCUs 112
Figure 89: Setting vehicle signals at remote information provider 112
Figure 90: Event generation at remote information provider 113
Figure 91: Only one client PCU may supply GPS information 114
Figure 92: Event generation at remote information provider 114
Figure 93: Only one client PCU may supply a specific communication protocol 116
Figure 94: Configuration of the IBIS (VDV300) protocol vial remote information provider 117
Figure 95: Configuring digital outputs via remote information provider 118
Figure 96: Automatic configuration of the Wi-Fi network interface 120
Figure 97: Manual configuration of the Wi-Fi network interface 121
Figure 98: Configuration of the J1708/J1587 communication protocol 122
Figure 99: Configuration of the IBIS (VDV300) protocol 123
Figure 100: Addressing doors in the IBIS VDV300 bus by door numbers 124
Figure 101: Configuration of the IBIS-VDV300 door client function 125
Figure 102: Configuration of the DCP Level 1 protocol 126

Figure 103: Configuration of the Digital Outputs 127
Figure 104: Generation of the passenger detection signal 128
Figure 105: Timing of the counting pulse signal 129
Figure 106: Downloading a configuration as XML file 130
Figure 107: The configuration is shown in a new browser window 130
Figure 108: Loading a configuration from an XML file 131
Figure 109: Check XML configuration 132
Figure 110: Validating a single configuration file 133
Figure 111: Uploading and saving a consist configuration package 133
Figure 112: Downloading a consist configuration package 134
Figure 113: State of the configuration plug 137
Figure 114: Starting a firmware update 138
Figure 115: Status information and requests during a firmware update 138
Figure 116: Script file template for firmware update 139
Figure 117: Log viewer 143
Figure 118: Creating an error report 144
Figure 119: Authorization dialog box 145
Figure 120: Live Counting View 146
Figure 121: Device information (example) 147
Figure 122: View of the current associated client PCUs 153
Figure 123: Testing the GSM status 154
Figure 124: Scanning for available Wi-Fi network stations 155
Figure 125: Testing the Wi-Fi status 155
Figure 126: Confirm to start testing 156
Figure 127: Transmission of a test file via FTP (processing) 156
Figure 128: Transmission of a test file via FTP (done) 156
Figure 129: Confirm transmission of test data via SMTP 157
Figure 130: Transmission of test data via SMTP (processing) 157
Figure 131: Transmission of a test data via SMTP (done) 157
Figure 132: Confirm transmission of test data via HTTP 157
Figure 133: Transmission of test data via HTTP (processing) 158
Figure 134: Transmission of a test data via HTTP (done) 158
Figure 135: Setting the logging level to test IBIS communication 158
Figure 136: Odometer details (left: automatic calibration, right: when a value is configured) 159
Figure 137: Screenshot of "ping" 163

Figure 138: Screenshot of Wireshark 163
Figure 139: Starting the expert mode 164
Figure 140: Error message during configuration saving 165
Figure 141: Lines which contain errors 165
Figure 142: Drawing PCU-200 IP40 surface-mounted housing (metal shell) 168
Figure 143: Drawing PCU-200 IP54 surface-mounted housing 169
Figure 144: Drawing PCU-200 IP40 rack housing 169
Figure 145: Block diagram 170

List of tables

Table 1: Models without LEDs for digital inputs/outputs (G1) 17
Table 2: Models with LEDs for digital inputs/outputs (G2) 18
Table 3: Models with basic and optional additional functions 20
Table 4: Main connector pinning (X01) 26
Table 5: Main connector pinning (X02) 27
Table 6: Connecting set for main connector (X01, X02) 27
Table 7: Digital Inputs IN1-IN4: Electrical Properties 28
Table 8: Odometer Input IN5: Electrical Properties 29
Table 9: SSL connector pinning 32
Table 10: Ethernet connector pinning M12 33
Table 11: Ethernet connector pinning RJ45 33
Table 12: Rear connector pinning X10 35
Table 13: Rear connector pinning X11 35
Table 14: Connecting set X10, X11 36
Table 15: IBIS wires coding 36
Table 16: Digital Outputs: Electrical Properties 38
Table 17: Digital input IN6 and IN7: Electrical Properties 39
Table 18: Digital Input 8: Electrical Properties 39
Table 19: Overview of status indicators 41
Table 20: SST-100 connector pinning 42
Table 21: Electrical data SST-100 44
Table 22: Mechanical data SST-100 44
Table 23: Environmental data SST-100 44
Table 24: Trouble shooting SST-100 44
Table 25: Ordering information SST-100 44
Table 26: PDR-100 connector pinning 45
Table 27: Electrical data PDR-100 47
Table 28: Mechanical data PDR-100 47
Table 29: Environmental data PDR-100 48
Table 30: Ordering information PDR-100 48
Table 31: Via FTP accessible directories of the PCU 83
Table 32: Directories at the remote FTP server 85
Table 33: Directories at the remote FTP server – Example: Rawdata and scripting directories with different directory structure 85

Table 34: Directories at the remote FTP server – Example: Storage of all data in the same root path 85
Table 35: Profile commands in HTTP client configuration 88
Table 36: Status of certificate file 90
Table 37: Default values for data recording in mobile systems 95
Table 38: Keys for the recording profile 98
Table 39: Examples for key-value pairs 99
Table 40: Default values for data recording in stationary systems 100
Table 41: Parameters controlling the generation of live tracking messages at a station 102
Table 42: Parameter controlling the generation of live tracking messages when the vehicle moves to the next station 102
Table 43: Parameter controlling the generation of live tracking messages when the vehicle is out of operation 102
Table 44: Send interval parameter for live diagnostics 104
Table 45: Start delay parameter for live diagnostics 104
Table 46: Check interval parameter for live diagnostics 104
Table 47: Inversion behavior of digital output 118
Table 48: Inversion behavior of a digital output 127
Table 49: Log entry elements 144
Table 50: Live Counting View – Displayed information for a door 146
Table 51: Live Device Status – Displayed information for a door 148
Table 52: Diagnostic Messages 152
Table 53: Explanation of the variable content of Diagnostic Messages 152
Table 54: Device Information – Displayed information for a client PCU 154
Table 55: Morse codes of the error LED 160
Table 56: Trouble shooting 162
Table 57: Electrical data PCU-200 166
Table 58: Mechanical data PCU-200 166
Table 59: Environmental data PCU-200 166
Table 60: Timing characteristics used by PCU communication services 168
Table 61: Glossary 172

1 Introduction PCU-200 series

The PCU (Passenger Counting Unit) is the central control and counting unit in DILAX counting systems. The PCU collects data from infrared sensors and digital inputs and converts the received information into actual numbers of passengers or people leaving or entering an area. Depending on the model, GPS position determination as well as communication via GSM, WLAN or wire-bound (Ethernet) is possible.

This manual contains information required for the installation, configuration, maintenance, and troubleshooting of the models of the PCU-200 series for use by technicians.

Note: This manual is common for all models of the PCU-200 series and its variants existing at the time of manual creation. The models are grouped. They can be equipped with LEDs for digital inputs and outputs or they don't have these LEDs. It is marked when features are only valid for one model group. You get a clear overview of the models on page 17.

The functionalities described in this Product Manual refer to firmware version 1.28.0.

1.1 Architecture

The PCU-200 series is designed for mobile systems and, with firmware version 1.5, also for stationary systems. For stationary systems, the models act as a master. For mobile systems the models can act as master or client.

The client PCU collects the counting results but cannot send data to other devices or applications. Counting results can be read from a client PCU by another PCU acting as master or by an on-board computer via Ethernet. The PCU-210 and the PCU-220 are intended to act as client.

The master PCU enables data transfer to the data management and reporting software via Ethernet, or wireless communication. All events (door status, counting data) can be monitored via a web interface. The PCU-230 and PCU-250 are intended to act as master.

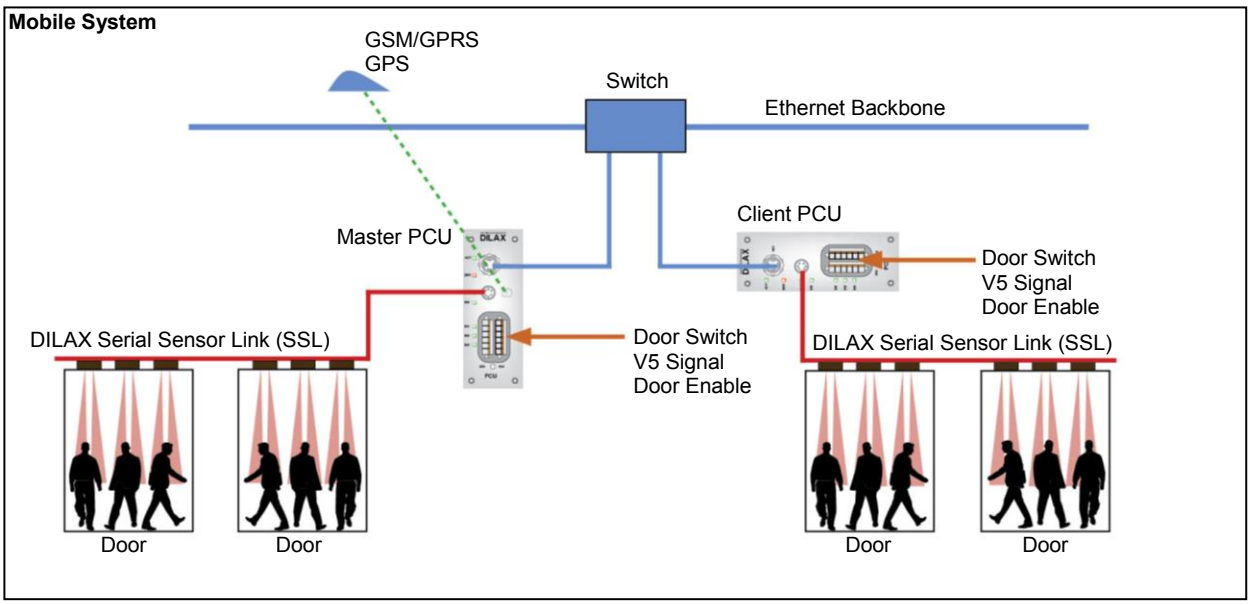


Figure 1: Master/client configuration of mobile systems

1.2 Models

The models of the PCU-200 series allow a flexible compilation of different functions to individual scenarios. They are available in variable variations. Overview of the PCU-200 series models with basic functions:

- PCU-210 with digital inputs and Ethernet interface
- PCU-220 with digital inputs, Ethernet interface, optional digital outputs and optional GPS receiver
- PCU-230 with digital inputs, integrated module for wireless data transfer via GSM/GPRS or WLAN, integrated GPS receiver and Ethernet interface P1. 1.10.6.1.3, P1. 1.10.6.1.4
- PCU-250 with digital inputs, digital outputs, module for wireless data transfer via GSM/GPRS or WLAN, integrated GPS receiver and Ethernet interface

Apart from basic functions, optional functions (e.g. integrated switch, second Ethernet interface) and different housing variations are available.

Overview of housing variations:

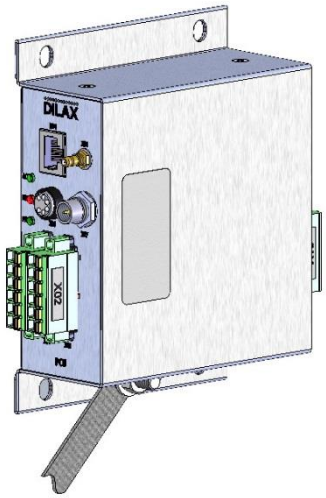


Figure 2: IP40 surface-mounted housing (metal shell)

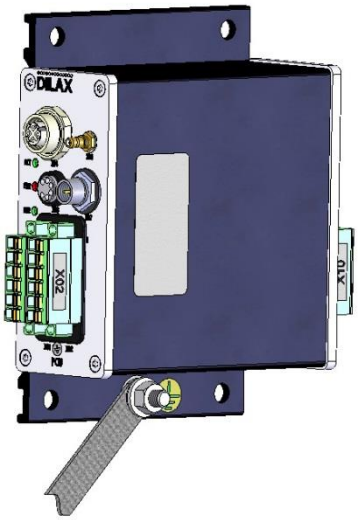


Figure 3: IP54 surface-mounted housing

Figure 4: IP40 rack housing

Models and variations described in this Product Manual

The models of the PCU-200 series are continuously improved and adapted to the market's requirements. They can be equipped with additional LEDs for digital inputs and outputs or they don't have these LEDs. The Product Manual applies for the models listed below:

Models without LEDs for digital inputs/outputs
(referenced in the Product Manual with group: **G1**)

PCU-210	
000.202.231.100	PCU-210 RJ45 IP40
000.202.231.200	PCU-210 M12 IP40
000.202.231.201	PCU-210 M12 IP40 Configuration Plug
000.202.231.504	PCU-210 M12 IP40 Ethernet-Switch RJ45 Rack 10TE
000.202.231.700	PCU-210 M12 IP54
000.202.231.701-B	PCU-210 M12 IP54 C-Plug
000.202.231.701-C	PCU-210 M12 IP54 C-Plug

PCU-230	
000.202.220.231	PCU-230 RJ45 WLAN IP40
000.202.235.110	PCU-230 RJ45 GSM IP40, Europe
000.202.235.140	PCU-230 RJ45 WLAN IP40, USA
000.202.235.150-B	PCU-230 RJ45 WLAN IP40
000.202.235.210	PCU-230 M12 GSM IP40, Europe
000.202.235.434	PCU-230 RJ45 WLAN IP40 Ethernet-Switch RJ45 Rack 10TE, Europe
000.202.235.440	PCU-230 RJ45 WLAN IP40 Rack 10TE, USA
000.202.235.444	PCU-230 RJ45 WLAN IP40 Ethernet-Switch RJ45 Rack 10TE, USA

PCU-250	
000.202.237.210	PCU-250 M12 GSM IP40, Europe
000.202.237.250	PCU-250 M12 WLAN IP40
000.202.237.410	PCU-250 RJ45 GSM IP40 Rack 10TE, Europe
000.202.237.414	PCU-250 RJ45 GSM IP40 Ethernet-Switch RJ45 Rack 10TE, Europe
000.202.237.450	PCU-250 RJ45 WLAN IP40 Rack 10TE
000.202.237.710	PCU-250 M12 GSM IP54, Europe

Table 1: Models without LEDs for digital inputs/outputs (G1)

Note: Table 1 lists all models of the PCU-200 series which already have been distributed by DILAX. Some of the listed models are no longer available for sale but only for orders of replacement parts.

In the context of projects, use the current sales and price lists for orders. Please ask your DILAX contact person in case of doubt.

Models with LEDs for digital inputs/outputs (referenced in the Product Manual with group: G2)	
PCU-210	
000.202.231.100-D	PCU-210 RJ45 IP40
000.202.231.200-D	PCU-210 M12 IP40
000.202.231.201-D	PCU-210 M12 IP40 Configuration Plug
000.202.231.202	PCU-210 M12 IP40 Ethernet-Switch M12
000.202.231.203-D	PCU-210 M12 IP40 C-Plug Switch M12
000.202.231.501-B	PCU-210 M12 IP40 C-Plug Rack 10TE
000.202.231.700-D	PCU-210 M12 IP54
000.202.231.701-D	PCU-210 M12 IP54 C-Plug
000.202.241.701-A	PCU-210 M12 IP54 C-Plug, 64MB
PCU-220	
000.202.233.209	PCU-220 M12 IP40 Switch RJ45, 2xPhoenix, RS-485 galv. isolated
000.202.233.509	PCU-220 M12 IP40 Switch RJ45, 2xPhoenix, RS-485 spec., Rack 10TE
000.202.233.562-A	PCU-220 M12 IP40 Switch M12, 2xPhoenix, IBIS, GPS, Rack 10TE
000.202.234.209	PCU-225 M12 IP40 Switch RJ45, D-SUB9 Interface, 2xPhoenix, RS-485 spec
000.202.233.260-A	PCU-220 M12 IP40 GPS
PCU-230	
000.202.235.110-D	PCU-230 RJ45 GSM IP40
000.202.235.150-D/E	PCU-230 RJ45 WLAN IP40
000.202.235.180-A	PCU-230 RJ45 3G IP40
PCU-250	
000.202.237.110	PCU-250 RJ45 GSM IP40
000.202.237.110-D	PCU-250 RJ45 GSM IP40
000.202.237.119	PCU-250 RJ45 GSM IP40, 12-32V DC
000.202.237.150-D/E	PCU-250 RJ45 WLAN IP40
000.202.237.211	PCU-250 M12 GSM IP40 Configuration Plug
000.202.237.212-D	PCU-250 M12 GSM IP40 Switch M12
000.202.237.213-D	PCU-250 M12 GSM IP40 C-Plug Switch M12
000.202.237.218	PCU-250 M12 GSM IP40, IBIS Recording Adapter
000.202.237.250-D/E	PCU-250 M12 WLAN IP40
000.202.237.258	PCU-250 M12 WLAN IP40, IBIS Recording Adapter
000.202.237.259	PCU-250 M12 WLAN IP40, RS-485 spez.
000.202.237.277-A	PCU-250 M12 GSM IP40 Switch M12; GLONASS, BOB
000.202.237.410-D	PCU-250 RJ45 GSM IP40 Rack 10TE, Europa
000.202.237.412-D	PCU-250 RJ45 GSM IP40 Ethernet-Switch M12 Rack 10TE
000.202.237.450-D/E	PCU-250 RJ45 WLAN IP40 Rack 10TE
000.202.237.513-D	PCU-250 M12 GSM IP40 C-Plug Ethernet-Switch M12 Rack 10TE
000.202.237.180-A	PCU-250 RJ45 3G IP40
000.202.237.283-A	PCU-250 M12 3G IP40 C-Plug Switch M12
000.202.237.480-A	PCU-250 RJ45 3G IP40 Rack 10TE

Table 2: Models with LEDs for digital inputs/outputs (G2)

Note: Table 2 lists all models of the PCU-200 series which already have been distributed by DILAX. Some of the listed models are no longer available for sale but only for orders of replacement parts.

In the context of projects, use the current sales and price lists for orders. Please ask your DILAX contact person in case of doubt.

	PCU-210		PCU-220	PCU-230		PCU-250	
	G1 [6]	G2 [6]	G2 [6]	G1 [6]	G2 [6]	G1 [6]	G2 [6]
Power supply PCU							
24 VDC power supply	x	x	x	x	x	x	x
12 VDC power supply							x [9]
General operating interfaces							
front	x	x	x	x	x	x	x
rear			x			x	x
Digital inputs [1]							
front	5	5	5	5	5	5	5
rear (option)			3			3	3
Digital outputs							
rear (option)			4			4	4
Ethernet interface (front)							
M12 or RJ45	x	x	x	x	x	x	x
Serial sensor link – ES-12 for optical sensors							
max. number of SSL-elements that can be connected	12	16 [7]	16 [7]	12	16 [7]	12	16 [7]
Network							
J1708/J1587	x	x	x		x		x
RS485 [4]			x				x
IBIS VDV300			x				x
Wireless communication							
WLAN [2]				x	x	x	x
GSM/GPRS incl. SIM card slot [2]				x	x	x	x
UMTS/3G incl. SIM card slot					x		
Satellite-based navigation system NAVSTAR GPS			(x) [10]	x	x	x	x
Satellite-based navigation system GLONASS							x
LED indicators							
Ethernet (front)	x	x	x	x	x	x	x
Error (front)	x	x	x	x	x	x	x
Power (front)	x	x	x	x	x	x	x
Digital inputs 1 to 4 (front)		x	x		x		x
Housing							
IP40 surface-mounted housing (metal shell) [3]	x	x	x	x	x	x	x
IP40 rack housing [3]	x	x	x	x	x	x	x
IP54 surface-mounted housing [3]	x	x	x	x	x	x	x
Optional additional functions (on request)							
2 port Ethernet switch (M12 or RJ45 on the rear)	x	x	x			x	x
LED indicator on the rear (Ethernet and Power, switch variant)		x	x				x
Isolated RS485 interface (1000V) – J1708 not available		x	x		x		x
5 V power supply up to 500 mA and USB on the rear for DILAX ESL [8]		x	x		x		x
Configuration plug SST-100 [8]	x	x	x	x	x	x	x
Second IBIS receive channel			x		x		x
Pull-Down Resistor PDR-100	x	x	x	x	x	x	x

Table 3: Models with basic and optional additional functions

1) front: 4 digital inputs via opto couplers, 1 digital input (referenced to power ground!) with software configurable pull-up/pull-down function, 1 ignition input for follow-up control
rear: 1 freely electrically configurable digital input (opto coupler), 2 high impedance digital inputs, one of them can be configured by software with a pull-up or pull-down, and usage as odometer input
2) Selective: WLAN or GSM
3) Selective: IP40, IP40 rack or IP54
4) Optional: Replaces J1708 interface
5) Optional: Replaces J1708 interface
6) See page 17 for information about the groups G1 and G2
7) To support 16 sensors, at least firmware version 1.9.0. must be installed on the models of this group.
8) The usage of the Configuration Plug SST-100, DILAX Extended Sensor Link ESL.
9) Selective: 12 V_{DC} or 24 V_{DC}
10) Only available for model 000.202.233.562-A

1.3 Key features

General:

- CE, EN 50155 compliant, e1/E1
- RoHS compliant
- Wall or rack mounting

Supported Ethernet Protocols:

Physical Layer: IEEE 802.3 Ethernet

- 100BASE-TX (100 MBit/s, full- or half-duplex)
- 10BASE-T (10 MBit/s, full- or half-duplex)
- Industrial Ethernet M12-D connectors
- MDI/MDI-X crossover detection

Network layer:

- IP (IPv4)
- ARP, ICMP, IGMP

Transport Layer:

- UDP, TCP

Application Layer:

- DHCP
- SNTP, SMTP
- HTTP, FTP
- DILAX Counting Protocol Level 2/3 (UDP/HTTP)

Further protocols:

- J1708/J1587
- IBIS (VDV300) active or passive
- DCP L1 (RS485)
- DILAX Extended Sensor Link (ESL, via DSN)

Counting:

- 1 supported SSL bus
- Supply of power to the SSL elements (sensors and digital inputs) via SSL bus from the PCU
- Max. 12 (G1) or 16 (G2) SSL elements (infrared sensors, digital sensors)
- At up to 6 different doors
- Max. total length of SSL: 30 m (G1) or 40 m (G2)
- Max. length of SSL between two sensors/SSL elements: 10 m
- On-board digital in- and outputs
- Counting can be activated/deactivated in consideration of certain events (e.g. door status)
- Counting events (IN/OUT) per door and per vehicle
- The counters can be monitored and reset via HTTP web interface.
- Counting results can be transmitted autonomously to an FTP server for analyzing.
- Counting and additional data can be sent in real-time via http directly to server (DILAX DRP, DCP L3)

System Log:

- Stored in RAM of PCU
- Priorities: Debug, Informational, Warning, Error, Fatal
- Error messages can be sent automatically by e-mail

Not all functions are available at all models and variations. See page 17 onwards for information about the groups G1 and G2 and possible functions.

P1. 1.10.5.2

2 Hardware Installation

2.1 Mechanical Mounting Instructions

The IP40 and IP54 housing variations for wall assembly vary slightly. However, they share the same dimension and position of the mounting holes (four M6 mounting holes). The rack variations of the PCU are intended to be used in racks and therefore no mounting holes are necessary.

On the front a clearance of 120 mm has to be planned for mounting of the connectors. The clearance on the rear depends on the variation, see Figure 5.

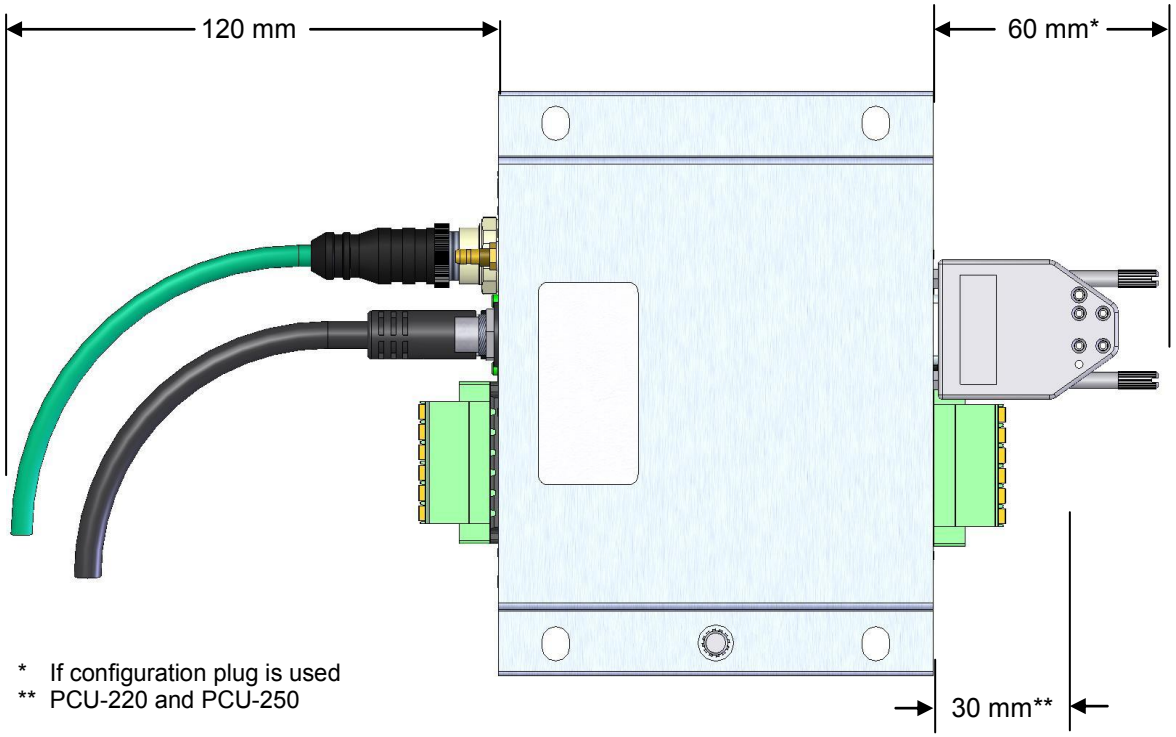


Figure 5: Minimum distances to be considered for installation

2.2 Power Consumption in Standby Mode

When the PCU is connected to the board power of the vehicle (X01-5) and started or shut down via ignition or the set-up/out-of-operation signal (X01-6), the PCU goes automatically in standby mode.

When the PCU is in standby mode, it has a power consumption smaller than 0.1 W at 24 V supply voltage.

Note: The terms standby, sleep and suspend mode are often used synonymously. It is the identic state at which data is stored in the device's RAM. This mode differs from the hibernation mode at which data is not stored in RAM but on a non-volatile memory (e.g. SSD, HDD).

2.3 Grounding concept

- **Chassis GND:** For best EMC behavior the PCU chassis is capacitive coupled to internal circuitry ground. In terms of DC, the PCU chassis is isolated. Chassis ground is connected via a M6 grounding stud, see Figure 6 and Figure 7.

- **SSL shield:** SSL shield is connected to circuit GND inside of the PCU. It is fed through the sensors/inputs up to the last sensor in the SSL and left open at the end.
- **DILAX LAN shield:** The shield of the DILAX LAN interface can be connected to the PCU chassis via pin 1 (X01).
- **Ethernet shield:** The M12 Ethernet jack is hardwired to chassis but DC-isolated from internal circuitry ground.

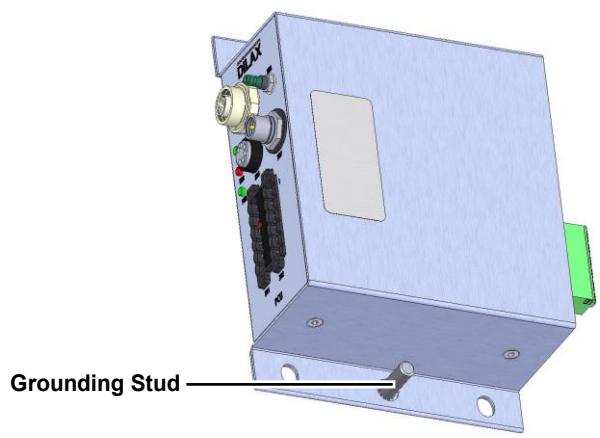


Figure 6: IP40 housing grounding stud location

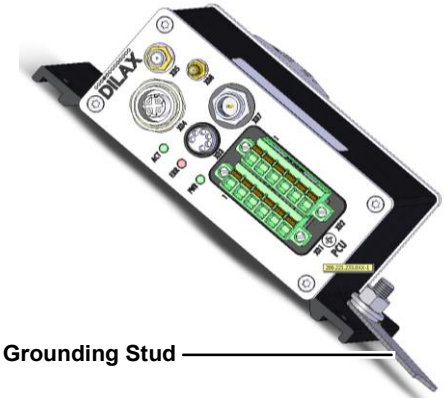


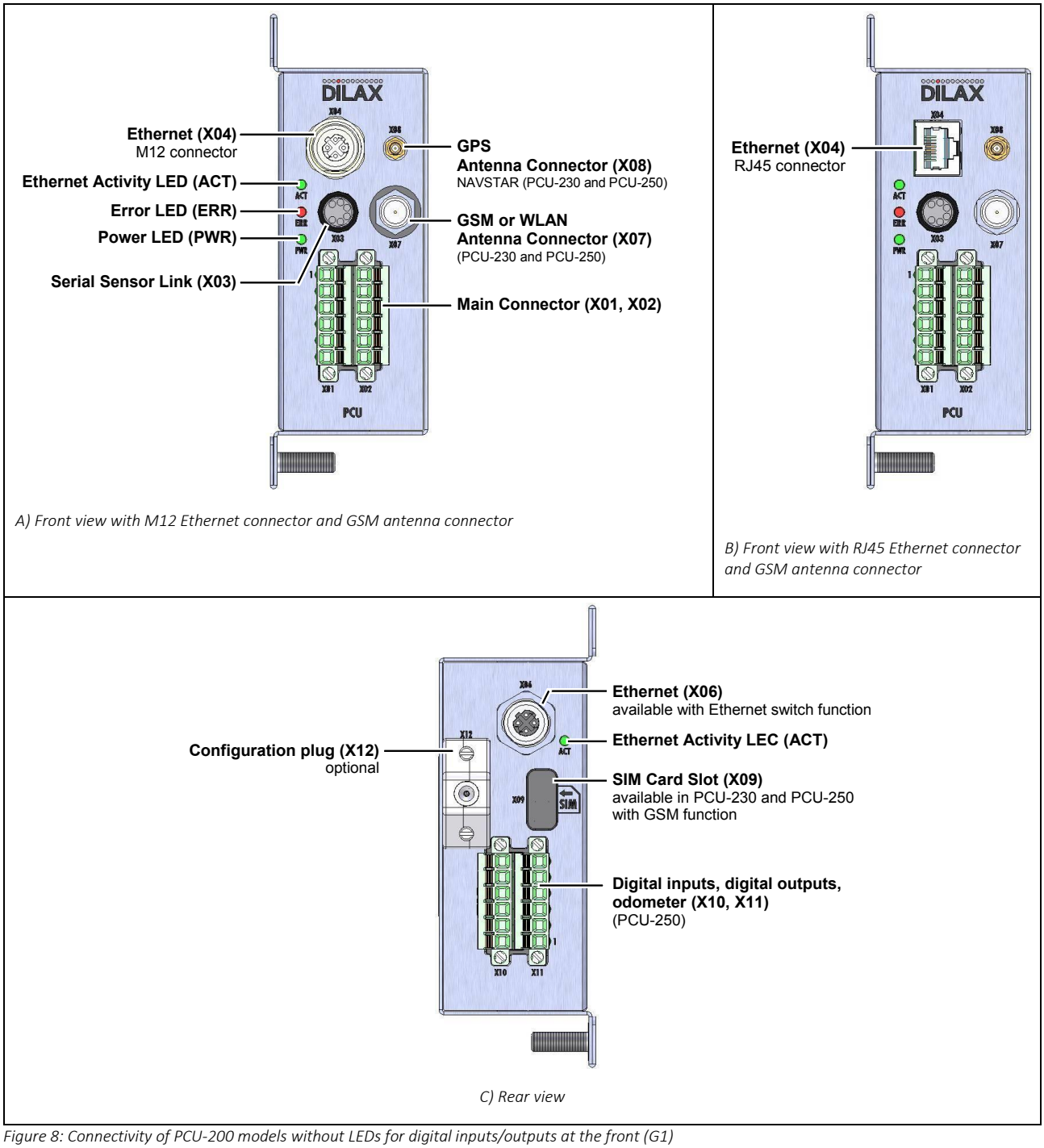
Figure 7: IP54 housing grounding stud location

Note: Chassis GND and signal ground are always separated (potential separation) if X04 is designed as M12 version.

2.4 Connectivity and Signal Description

2.4.1 PCU-200 Models without LEDs for digital inputs/outputs (G1)

The figures show a full-configured PCU-200 model (two Ethernet interfaces, interfaces for GSM, GPS antennas and configuration plug SST-100, SIM card slot and additional digital in- and outputs on the rear). Please note that the different PCU models are equipped with different interfaces.



A) Front view with M12 Ethernet connector and GSM antenna connector

B) Front view with RJ45 Ethernet connector and GSM antenna connector

C) Rear view

Figure 8: Connectivity of PCU-200 models without LEDs for digital inputs/outputs at the front (G1)

2.4.2 PCU-200 Models with LEDs for digital inputs/outputs (G2)

The figures show a full-configured PCU-200 model (two Ethernet interfaces, interfaces for GSM, GPS antennas and configuration plug SST-100, SIM card slot and additional digital in- and outputs on the rear). Please note that the different PCU models are equipped with different interfaces.

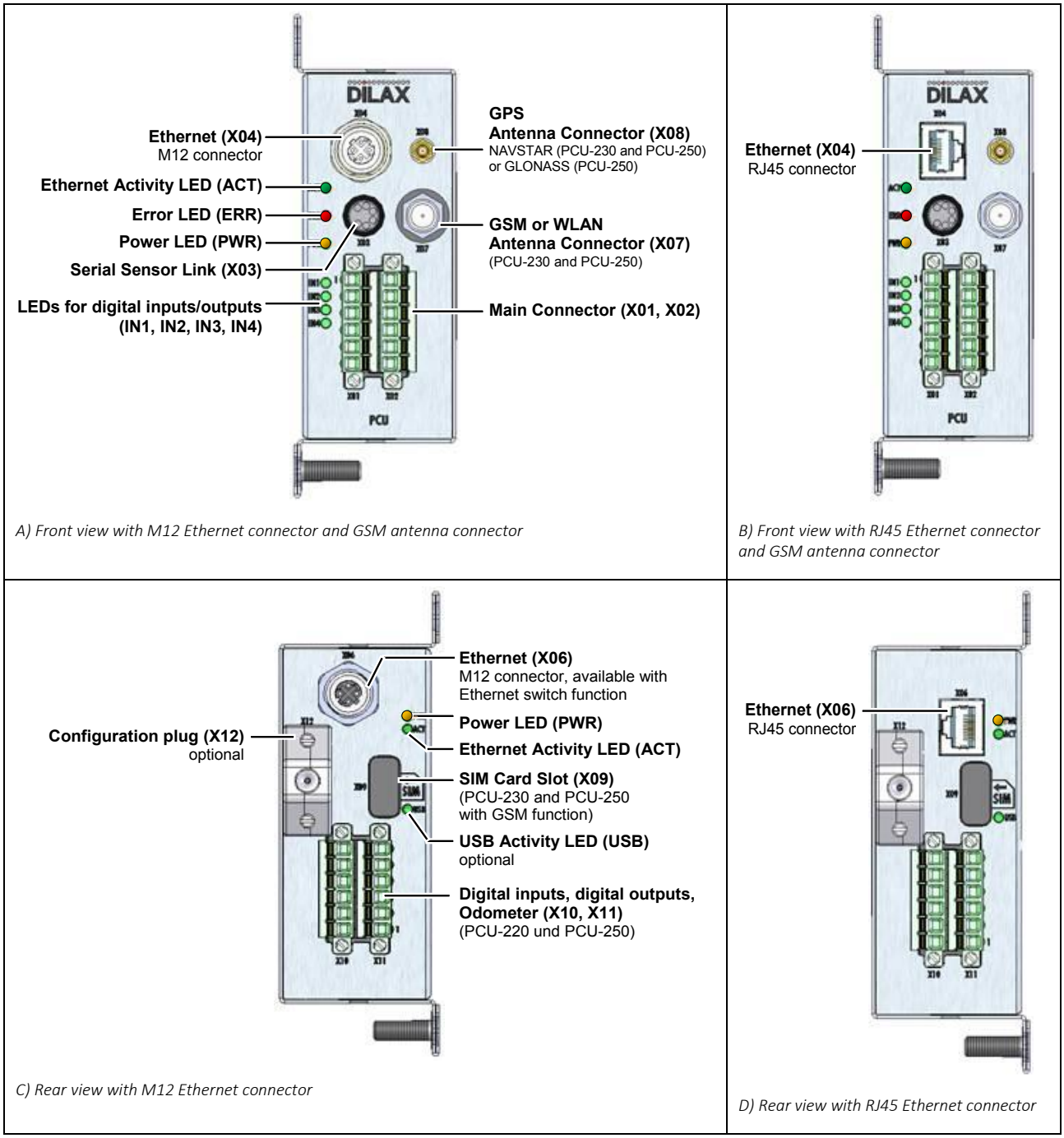


Figure 9: Connectivity of PCU-200 models with LEDs for digital inputs/outputs at the front (G2)

2.4.3 Main Connectors X01 and X02 (Power Supply, DILAX LAN, Digital Inputs)

Valid for:

☒ PCU-210 (G1)	☒ PCU-220(G2)	☒ PCU-230 (G1)	☒ PCU-250 (G1)
☒ PCU-210 (G2)		☒ PCU-230 (G2)	☒ PCU-250 (G2)

See page 17 for information about the groups G1 and G2.

Power supply, digital inputs and ignition as well as DILAX LAN connections are made via the main connectors X01/X02, which is a single Phoenix CCDN 2.5/6-G1F P26 THR 2x6 pin socket.

Code riders secure a clear assignment (see Figure 10).

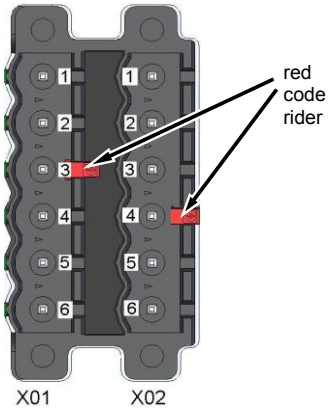


Figure 10: Main connector

Notes:

The PCU is supplied with power via pins X01-5 and X01-4.

Starting and shutting down of the PCU should be done via a separate switching signal at pin X01-6 (ignition signal for automotive or set-up/out-of-order signal for rail). When this switch signal is not available, pin X01-6 must be connected to pin X01-5 via a bridge or power for the PCU must be connected directly to pin X01-6. There must always be voltage at Pin X01-6 so that the PCU can be started.

At least once within 24 operation hours the power supply at pin X01-6 must be interrupted and the PCU must be restarted. Continuous operation of the PCU may lead to malfunctions!

The PCU must be electronically secured at installation. Therefore, use a slow blow fuse (max. 3 A).

<table>
<tr><th colspan="10">X01</th></tr>
<tr><th>Pin</th><th>Signal</th><th>I/O</th><th colspan="7">Level</th></tr>
<tr><td>1</td><td>CHASSIS GROUND</td><td></td><td colspan="7">Connected to housing potential, 500V_{DC} isolated from internal electronics.</td></tr>
<tr><td rowspan="3">2</td><td rowspan="3">LAN-A (RS-485 or J1708 level A (+))
or
IBIS monitor connector (WBED, option)</td><td rowspan="3">I/O</td><td colspan="2">PCU-210</td><td>PCU-220</td><td colspan="2">PCU-230</td><td colspan="2">PCU-250</td></tr>
<tr><td>G1</td><td>G2</td><td>G2</td><td>G1</td><td>G2</td><td>G1</td><td>G2</td></tr>
<tr><td>LAN-A</td><td>LAN-A
IBIS monitor</td><td>LAN-A
IBIS monitor</td><td>LAN-A</td><td>LAN-A
IBIS monitor</td><td>LAN-A</td><td>LAN-A
IBIS monitor</td></tr>
<tr><td colspan="8">LAN-A: RS-485 and J1708 can be configured separately or parallel.</td></tr>
<tr><td rowspan="3">3</td><td rowspan="3">LAN-B (RS-485 or J1708 level B (-))
or
IBIS monitor connector (WBME, option)</td><td rowspan="3">I/O</td><td colspan="2">PCU-210</td><td>PCU-220</td><td colspan="2">PCU-230</td><td colspan="2">PCU-250</td></tr>
<tr><td>G1</td><td>G2</td><td>G2</td><td>G1</td><td>G2</td><td>G1</td><td>G2</td></tr>
<tr><td>LAN-B</td><td>LAN-B
IBIS monitor</td><td>LAN-B
IBIS monitor</td><td>LAN-B</td><td>LAN-B
IBIS monitor</td><td>LAN-B</td><td>LAN-B
IBIS monitor</td></tr>
<tr><td colspan="8">LAN-B: RS-485 and J1708 can be configured separately or parallel.</td></tr>
<tr><td>4</td><td>GND</td><td>PWR</td><td colspan="7">0 V_{DC}</td></tr>
<tr><td>5</td><td>VIN</td><td>PWR</td><td colspan="7">16.8 – 45 V_{DC}</td></tr>
<tr><td>6</td><td>IGNITION (start/shut-down, must always be used)</td><td>I/PWR</td><td colspan="7">16.8 – 45 V_{DC}
Note: When there is no separate switching signal available, this pin must be connected to Pin 5 via a bridge or power supply must be connected directly to this pin. Ensure the PCU is disconnected from power supply and restarted at least once within 24 hours operation time.</td></tr>
</table>

Table 4: Main connector pinning (X01)

X02			
Pin	Signal	I/O	Level (max.)
1	IN1	I	60 V_{DC}
2	IN2	I	60 V_{DC}
3	IN3	I	60 V_{DC}
4	IN4	I	60 V_{DC}
5	IN- Common for IN1…IN4	I	60 V_{DC}
6	IN5 speedometer	I	50.4 V_{DC} Note: referenced to GND, not potential free! Freq: 20 KHz; 25%/75%

Table 5: Main connector pinning (X02)

The following connecting set (spring-cage plug FKCN 2.5/6 STF, code pin, code rider) is available for connection:

Model	Article no.
PCU-210 and PCU-230:	000.202.200.601
PCU-220 and PCU-250:	000.202.210.601

Table 6: Connecting set for main connector (X01, X02)

Note: The spring-cage plug FKCN 2.5/6 STF for the PCU-200 series is not a standard interface. DILAX uses a modified interface provided by the connecting set. Please always use the specific connectors together with code pin and code rider on the correct position.

2.4.3.1 Digital Inputs IN1-IN4

Every model of the PCU-200 series is equipped with 4 digital inputs which are isolated from the internal circuitry by opto couplers. The principle of the inputs is shown in Figure 11. Pin 5 of connector X02 is the common (-)pin to all 4 digital inputs.

If a voltage source is connected to the inputs, connect the negative side to common IN- (common ground) and the positive side to IN1, IN2, IN3 or IN4 respectively.

If dry contacts are connected to the digital inputs, the power supply or an external power supply may be used: connect GND to IN- and connect VCC to external dry contacts IN1 or IN2, IN3, IN4 (for connection examples see chapter 2.4.3.3).

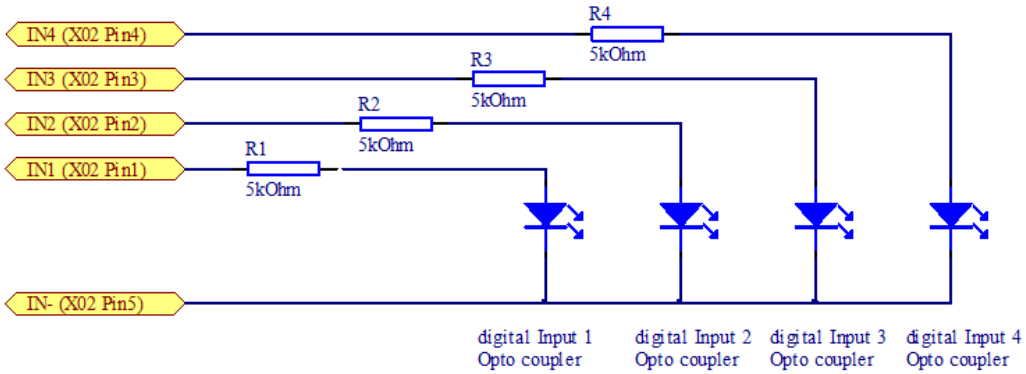


Figure 11: Principle of digital input circuit 1-4

Digital Inputs IN1-IN4: Electrical Properties

Maximum input voltage (between IN- and IN0, IN1 or IN2)	60 V
Maximum reverse voltage (between IN- and IN0, IN1 or IN2)	-60 V
Galvanic isolation	@ 500 VDC > 1 mega Ohm
High level input voltage	10 V...60 V
Low level input voltage	0...2.5 V
Input resistance	5 kOhm
Maximum switching frequency	10 Hz

Table 7: Digital Inputs IN1-IN4: Electrical Properties

Note: Digital inputs are usually used to detect the door status by door contacts. A correct detection of the door status (open, closed) and the opening duration are essential for the accurate operation of the automatic counting system. At doors with several segments the door contact must switch active when at least one segment is open. The basic behavior of the digital inputs (normally open NO, normally closed NC) can be configured in the PCU and inverted, if needed. The time period for counting between opening and closing the door can be configured (see chapter 3.7).

Recommendation: The door signals should be configured to have 24 V_{DC} (active, high level) at the digital inputs of the PCU when the doors are closed and 0 V_{DC} (inactive, low level) when the doors are open. This ensures that entering and leaving passengers are still counted even if the vehicle is standing still with switched off ignition (e.g. at final stops).

2.4.3.2 IN5 (Odometer Input for Driving Speed Calculation)

Input IN5 is reserved for the impulses from an odometer. For one counting event a rising edge from lower than 1.5 V to higher than 6.5 V is needed at IN5.

If necessary, a pull-up or pull-down resistor can be enabled (see 3.7 and 3.9). This may be necessary depending on the odometer signal generator. For further information, please read the manual of the odometer manufacturer.

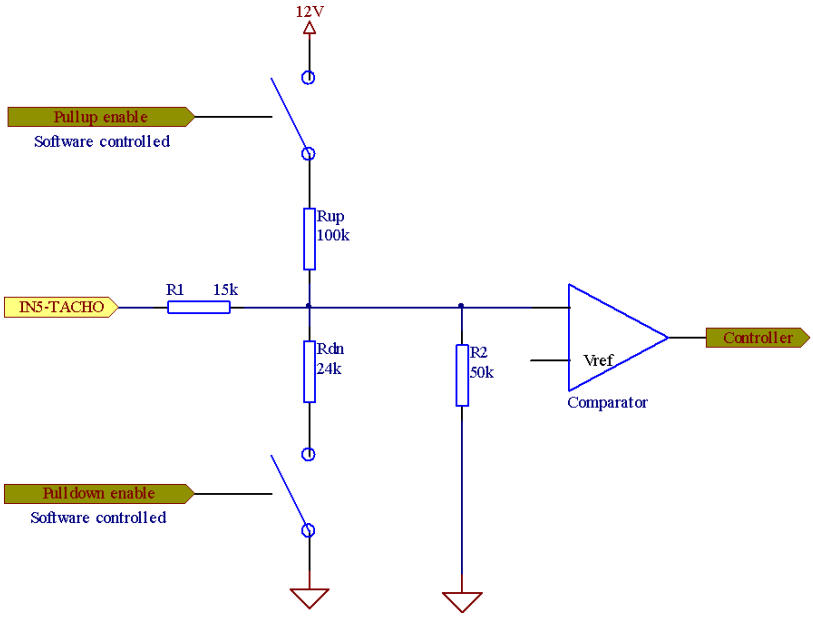


Figure 12: Principle of digital input circuit IN5

Odometer Input IN5: Electrical Properties

Maximum input voltage (reference: 0VDC PIN X01-4)	54 V
Input voltage high level	6.5 V...54 V
Input voltage low level	0...2.5 V
Input resistance (without active pull-up or pull-down resistor)	65 kOhm
Maximum switching frequency at maximum duty cycle	20 kHz at 25%/75%

Table 8: Odometer Input IN5: Electrical Properties

2.4.3.3 Wiring examples

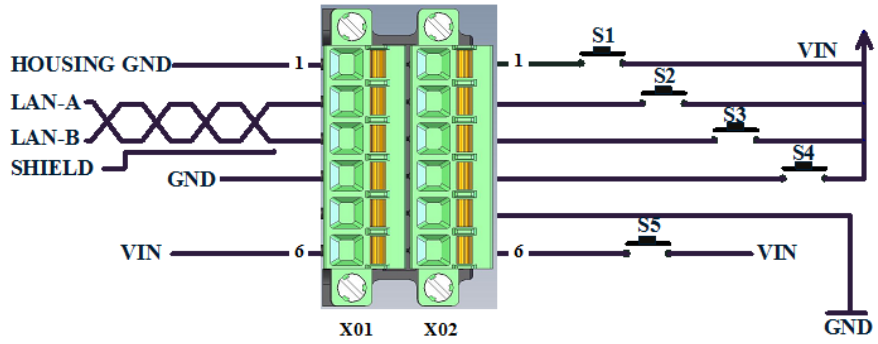


Figure 13 shows a typical wiring example with switching contacts S1-S4 and a power supply. Input "IN 5" (pin 6, X02) can also be used as a non-isolated input with PCU-GND reference. Alternatively, use pin 6 of X02 for pulsed odometer signals.

By applying a switching voltage or supply voltage to pin X01-6, the PCU is powered on/off.

Figure 13: Digital inputs with external contacts (door contacts)

Note: It is recommended to connect X01-5 to the positive (+) pole of the vehicle's battery (acc. DIN 72552 clamp 30*) and X01-6 to the vehicle's ignition or set-up/out-of-order signal (acc. DIN 72552 clamp 15*). When there is no separate switching available, power supply must directly be connected to pin X01-6 (see Figure 13).

Ensure the PCU is disconnected from power supply and restarted at least once within 24 hours operation time. Always secure the PCU electrically (see chapter 2.4.3).

** Clamp designations can differ depending on the vehicle type.*

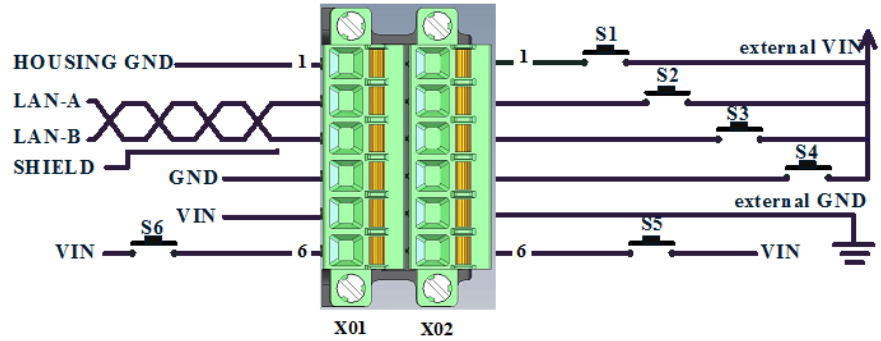


Figure 14 shows a typical wiring example with door contacts S1-S4 with a switching voltage for the digital inputs without reference potential to the PCU. S5 is used as non-isolated input with respect to the PCU-GND. Reference potential of S5 is GND. In this example, the ignition function is used.

The PCU is switched on and off via S6 (ignition or start-up/out-of-operation signal). During operation S6 must be closed. A power off delay (ignition shutdown delay) can be configured via the PCU's web interface.

Figure 14: DC switched isolated digital inputs (function ignition active and use of the 5th digital input with reference potential GND)

Note: For proper operation of the power off delay, VIN must always be supplied with power (battery of the vehicle). When the signal at the ignition input turns off, the PCU continues operating until the ignition shutdown delay expires. After that the PCU turns off.

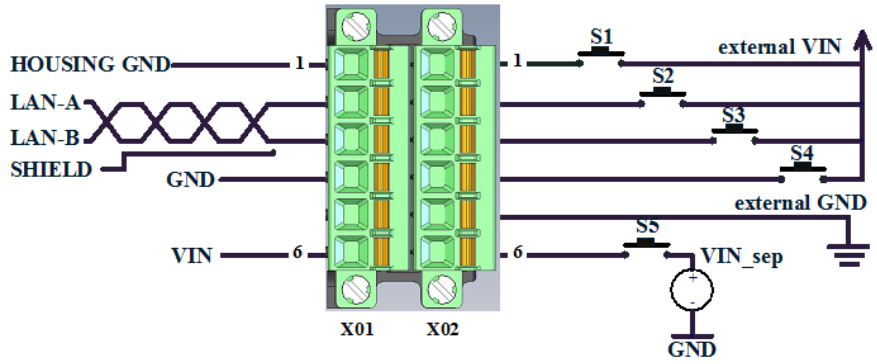


Figure 15: DC switched isolated digital inputs (without ignition)

Figure 15 shows a typical wiring example with DC switched digital inputs isolated from PCU-GND. S5 is also used as input to an external power source, but referenced to PCU GND (non-isolated).

By applying a switching voltage or supply voltage to pin X01-6, the PCU is powered on/off.

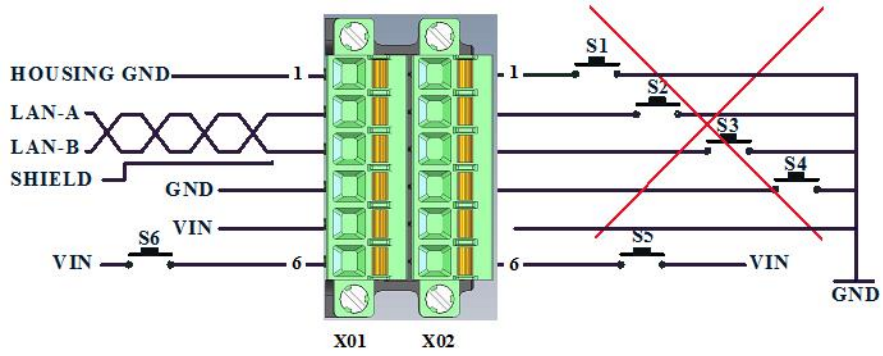


Figure 16: Example for an invalid wiring

The example in Figure 16 shows an invalid wiring of the digital inputs S1-S4.

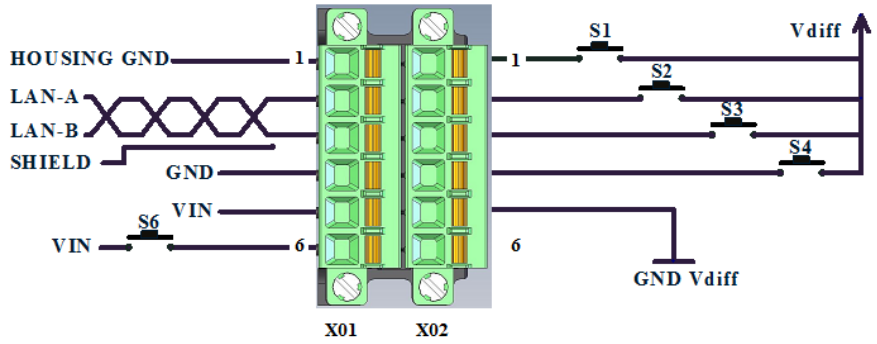


Figure 17: Digital inputs with different voltages

If a second voltage supply (Vdiff), which is independent of the main PCU supply voltage, is used for the digital inputs it must be connected as shown in Figure 17. Vdiff must be at a higher potential than GND Vdiff.

2.4.4 Serial Sensor Link SSL (X03)

Valid for:

☒ PCU-210 (G1)	☒ PCU-220 (G2)	☒ PCU-230 (G1)	☒ PCU-250 (G1)
☒ PCU-210 (G2)		☒ PCU-230 (G2)	☒ PCU-250 (G2)

See page 17 for information about the groups G1 and G2.

P1. 1.10.5.2 P1. 1.10.6.1.6

The SSL connector is a 6-pin ES-12 female. Infrared sensors and external inputs (INP) are connected to this connector via DILAX SSL cable.

Maximum number of devices that can be connected:	12 (G1)	or 16 (G2)
Maximum length of complete SSL bus:	30 m (G1)	or 40 m (G2)
Maximum length of SSL bus between two SSL devices:	10 m (G1 and G2)	

Make sure the SSL devices have a distribution as uniform as possible.

Pin	Signal	I/O	Level
1	Power Supply	PWR	12 V_{DC}
2	GND	PWR	0 V_{DC}
3	SSL-Shield		0 V_{DC}
4	SSL-Shield		0 V_{DC}
5	CLK OUT	O	+12 V_{DD} / 125 kHz
6	DATA IN	I	+12 V_{DD} / 125 kHz

Table 9: SSL connector pinning

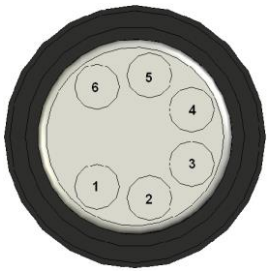


Figure 18: SSL connector

2.4.5 Ethernet ETH (X04, X06)

Valid for:

☒ PCU-210 (G1)	☒ PCU-220 (G2)	☒ PCU-230 (G1)	☒ PCU-250 (G1)
☒ PCU-210 (G2)		☒ PCU-230 (G2)	☒ PCU-250 (G2)

See page 17 for information about the groups G1 and G2.

The models are selectively available with Ethernet interfaces at the front (X04) or both front and rear side (X06) (coupling through internal switch). The interface is selectively available as RJ45 or M12 (recommendation: M12 interface because it is shock-proof). With these interfaces it is possible to connect several PCU devices in order to create master client systems (cascading).

Recommendation: It is recommended to connect X04 (front side) to vehicle Ethernet backbone and to use X06 (rear side) for service purposes.

Notes: Connection to Ethernet backbone is checked first on Interface X04 (front side).
If no link was detected, X06 (rear side) is checked.

Avoid a ring topology. This coupling of both interfaces X04 and X06 to the same switch would cause a switching loop which causes a network failure.

Interfaces X04 and X06 are galvanic isolated in both versions, RJ45 and M12.

P1. 1.10.5.2 P1. 1.10.6.1.6

2.4.5.1 M12 Ethernet connector

The M12 variant of the 10/100 BASE-T Ethernet interface is realized as d-coded M12 female connector with MDI/MDI-X crossover detection. For connections, use standard d-coded M12 male connectors. A DILAX Ethernet cable is used for connection (CAT5 cable 4 core twisted and shielded, 100 MBit/s fast Ethernet).

Pin	Signal	I/O	Level
1	TX+	O	see Ethernet-Specification IEEE 802-3
2	RX+	I	see Ethernet-Specification IEEE 802-3
3	TX-	O	see Ethernet-Specification IEEE 802-3
4	RX-	I	see Ethernet-Specification IEEE 802-3
	Shield	n/a	The housing of the M12 connector is connected to the PCU housing ground.

Table 10: Ethernet connector pinning M12

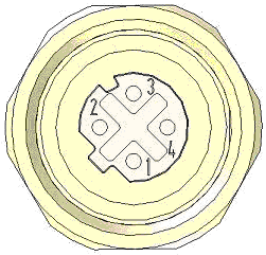


Figure 19: Ethernet connector M12

2.4.5.2 RJ45 Ethernet connector

The RJ45 variant of the 10/100 BASE-T Ethernet interface is realized as a RJ45 (8P8C) female connector. For connections, use standard RJ45 (8P8C) male connectors. Ethernet cable is used for connection (CAT5 cable 4 core twisted and shielded, 100 MBit/s fast Ethernet).

Pin	Signal	I/O	Level
1	TX+	O	see Ethernet-Specification IEEE 802-3
2	TX-	O	see Ethernet-Specification IEEE 802-3
3	RX+	I	see Ethernet-Specification IEEE 802-3
4	n/c	n/a	n/a
5	n/c	n/a	n/a
6	RX-	I	see Ethernet-Specification IEEE 802-3
7	n/c	n/a	n/a
8	n/c	n/a	n/a
	Shield	n/a	The housing of the RJ45 connector is connected to the PCU housing ground.

Table 11: Ethernet connector pinning RJ45

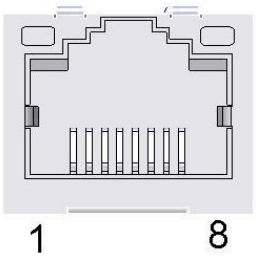


Figure 20: Ethernet connector RJ45

2.4.6 GSM/WLAN Antenna Connector (X07)

Valid for:

☐ PCU-210 (G1)	☐ PCU-220 (G2)	☒ PCU-230 (G1)	☒ PCU-250 (G1)
☐ PCU-210 (G2)		☒ PCU-230 (G2)	☒ PCU-250 (G2)

See page 17 for information about the groups G1 and G2.

Depending on the variation, the models of the PCU-200 series have an integrated GSM, UMTS, or WLAN module for wireless data transfer. The X07 interface for WLAN antennas is realized as SMA connector with external thread (female). The X07 interface for GSM antennas is realized as FME connector with internal thread (male).

2.4.7 GPS Antenna Connector (X08)

By default, the PCU has an internal GPS receiver supporting GPS NAVSTAR. However, specific models can have an internal GPS receiver supporting GPS NAVSTAR and GPS GLONASS.

P1. 1.10.5.2

P1. 1.10.6.1.6

GPS NAVSTAR valid for:

☐ PCU-210 (G1)	☒ PCU-220 (G2), only model	☒ PCU-230 (G1)	☒ PCU-250 (G1)
☐ PCU-210 (G2)	000.202.233.562-A	☒ PCU-230 (G2)	☒ PCU-250 (G2)

GPS GLONASS valid for:

☐ PCU-210 (G1)	☐ PCU-220 (G2)	☐ PCU-230 (G1)	☐ PCU-250 (G1)
☐ PCU-210 (G2)		☐ PCU-230 (G2)	☒ PCU-250 (G2)

See page 17 for information about the groups G1 and G2.

The X08 interface is only available for models with integrated GPS receiver module (NAVSTAR or GLONASS). It is an SMB reverse connector (male). The PCU can supply active GPS antennas with phantom power (3.3 VDC) via the X08 interface. This can be configured (activated/deactivated) in the web interface of the device. Default setting is "deactivated". Maximum current for antenna supply is 100 mA. It may not be exceeded.

Notes

In order to use GPS GLONASS, a GLONASS compatible antenna must be connected. Pure NAVSTAR GPS antennas cannot be used due to both navigation systems use different frequency bands. Multiband antennas can be used but have to be checked for their technical suitability first.

The X08 interface is internally galvanic isolated from chassis ground.

P1 1.10.6.1.4.

2.4.8 SIM Card Slot (X09)

Valid for:

☐ PCU-210 (G1)	☐ PCU-220 (G2)	☒ PCU-230 (G1)	☒ PCU-250 (G1)
☐ PCU-210 (G2)		☒ PCU-230 (G2)	☒ PCU-250 (G2)

See page 17 for information about the groups G1 and G2.

The SIM card slot is only available in models with GSM function.

The following SIM cards can be used:
(Measurements: length x width x thickness)

- ? **Mini-SIM** (ISO/IEC 7810:2003, ID-000)
  Measurements: 25 x 15 x 0,76 mm

The following formats are not supported:
(Measurements: length x width x thickness)

- ? **Full-size** (ISO/IEC 7810:2003, ID-1)
  Measurements: 85,6 x 53,98 x 0,76 mm
- ? **Micro SIM** (ETSI TS 102 221 V9.0.0, Mini-UICC)
  Measurements: 15 x 12 x 0,76 mm
- ✗ **Nano SIM** (ETSI TS 102 221, TS 102 221 V11.0.0)
  Measurements: 12,30 x 8,8 x 0,67 mm
- ? **Embedded** (JEDEC Design Guide 4.8 , SON-8)
  Measurements: 6 x 5 x < 1,0 mm

2.4.9 Rear Connectors X10 and X11 (Digital Outputs, Digital Inputs, Odometer)

Valid for:

☐ PCU-210 (G1)	☒ PCU-220 (G2)	☐ PCU-230 (G1)	☒ PCU-250 (G1)
☐ PCU-210 (G2)		☐ PCU-230 (G2)	☒ PCU-250 (G2)

See page 17 for information about the groups G1 and G2.

P1. 1.10.5.2 P1. 1.10.6.1.6

On the rear a second Phoenix connector can be available for interfacing 4 digital outputs and 3 digital inputs in different configurations. Type: Phoenix CCDN 2.5/6-G1F P26 THR 2x6-pin socket. Code riders secure a clear assignment (see Figure 21).

Note: In addition to further digital inputs and output interfaces X10/X11 offer the possibility to use the PCU as IBIS VDV300 client. This is a complete communication interface according to VDV300. It is not identical to the optional IBIS monitor interface at the front of the PCU! X10/X11 connector pinning is described in Table 12 and Table 13.

Take into account: When the VDV300 interface is used, the digital output 3 cannot be used and configured!

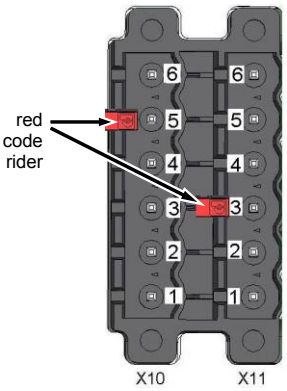


Figure 21: Rear connectors X10 and X11

X10			
Pin	**Signal**	**I/O**	**Level (max.)**
1	Digital Output 1	O	60 V_{DC}, max. 100 mA
2	Common Pin for Outputs 1 and 2	O	60 V_{DC}
3	Digital Output 2	O	60 V_{DC}, max. 100 mA
4	Digital Output 3	O	60 V_{DC}
5	Common Pin for Outputs 3 and 4	O	60 V_{DC} (IBIS-VDV300: WBME), max. 100 mA, RX-
6	Digital Output 4	O	60 V_{DC} (IBIS-VDV300: WBED) , max. 100 mA, RX+

Table 12: Rear connector pinning X10

X11			
Pin	**Signal**	**I/O**	**Level (max.)**
1	IN6	I	50.4 V_{DC} referenced to GND_{ISO}
2	IN7	I	50.4 V_{DC} referenced to GND_{ISO}
3	GND_{ISO}	PWR	Reference to V_{ISO} (isolated from internal electronics 500 V)
4	V_{ISO}	PWR	5 V_{DC} (isolated from internal electronics 500 V)
5	IN8-	I	60 V_{DC} (galvanic isolated from internal electronics 500 V – IBIS-VDV300: WBMS), TX-
6	IN8+	I	60 V_{DC} (galvanic isolated from internal electronics 500 V – IBIS-VDV300: WBSD), TX+

Table 13: Rear connector pinning X11

The following connecting set (spring-cage plug FKCN 2.5/6 STF, code pin, code rider) is available for connection:

Model	Article no.
PCU-210 and PCU-230:	000.202.200.601
PCU-220 and PCU-250:	000.202.210.601

Table 14: Connecting set X10, X11

Note: The spring-cage plug FKCN 2.5/6 STF for the PCU-200 series is not a standard plug. DILAX uses a modified plug provided by the connecting set.
Please always use the modified plug together with a code pin and code rider on the correct position.

2.4.9.1 IBIS-VDV300 Interface

The IBIS VDV300 vehicle bus is an onboard communication system for vehicles. Data is transferred via a 4-wire bus: one wire pair for request data (vehicle bus send), the second wire pair for response data (vehicle bus reception). The wire designations are always from the view of the vehicle bus master (IBIS controller unit). Within the IBIS vehicle bus the PCU is a peripheral device (client) which responds (WBE) to the data requests of the IBIS controller unit (WBS).

The PCU can be used as passive or active IBIS peripheral device:

- **Passive (data logger):** The PCU reads and processes data on the IBIS vehicle bus. It does not respond as IBIS client on requests of the IBIS controller unit. The wires WBSD and WBMS must be connected to the PCU for this behavior.
- **Active (IBIS client):** The PCU works as a data logger and, in addition, responds as APC device on requests of the IBIS controller unit according to the VDV300 specification. The wires WBSD, WBMS and WBED, WBME must be connected to the PCU for this behavior.

Furthermore the data telegrams which should be considered must be configured in the PCU.

Designation and color codes:

IBIS code	Designation (view of the controller unit)	PCU contact	Data (view of the controller unit)	Color code
WBSD	Vehicle Bus Send Data (to PCU, receiving data)	IN8+ (X11 pin 6)	TX+	White
WBMS	Vehicle Bus Send Ground	IN8- (X11 pin 5)	TX-	Brown
WBED	Vehicle Bus Receive Data (from PCU)	OUT 4 (X10 pin 6)	RX+	Yellow
WBME	Vehicle Bus Receive Ground	OUT 3/4 common (X10 pin 5)	RX-	Green

Table 15: IBIS wires coding

2.4.9.2 Digital Outputs

4 digital outputs are available which are isolated from the internal circuitry by opto couplers. The principle of the outputs is shown in Figure 22 (protection diodes are not shown).

Digital output 1, 2 and 3 have the same internal switch. They are not polarized and have a maximum current of 100 mA. Digital output 4 uses an NPN Darlington transistor for switching. It is polarized with pin 6 having a higher potential than pin 5 (emitter). Digital outputs 1 and 2 share the reference pin X10 pin 2 and the digital outputs 3 and 4 share the reference pin X10 pin 5.

Note: Digital output 4 is not short circuit protected! Do not apply reverse voltage.

When pins 5 and 6 of the X10/X11 interface of the PCU are used for IBIS VDV300 communication, these pins cannot be used in parallel as digital outputs 3 and 4 (double assignment).

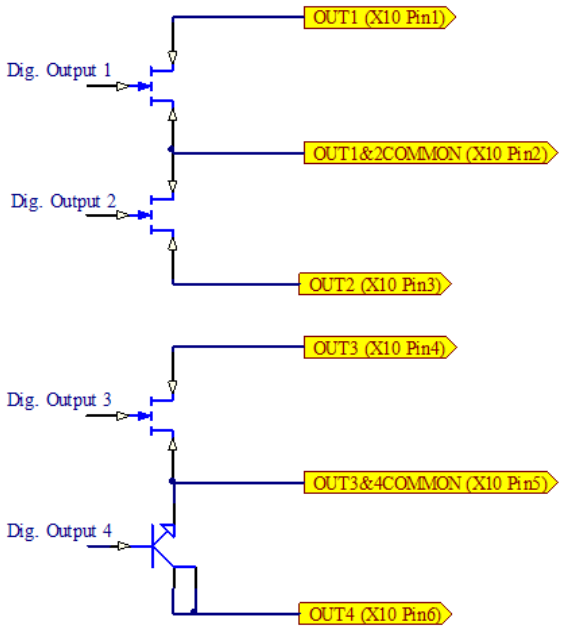


Figure 22: Principle of digital output circuit 1-4

Digital Outputs: Electrical Properties

Maximum voltage (between terminals) outputs 1, 2 and 3	60 V_{DC} (negative or positive, AC or DC operation possible)
Maximum voltage (between terminal 5 and 6) output 4	60 V_{DC} (do not apply reverse voltage)
Isolation	+/- 500 V_{DC}
Maximum current dig. outputs 1, 2 and 3	100 mA (negative or positive, AC or DC operation possible)
Maximum current dig. output 4	500 mA (do not apply reverse voltage)
Maximum switching frequency outputs 1, 2 and 3	10 Hz
Maximum switching frequency output 4	1200 Hz
On resistance	Max. 25 Ohm

Table 16: Digital Outputs: Electrical Properties

2.4.9.3 Digital Inputs 6 and 7

Two high impedance digital inputs are available which are isolated from the internal circuitry. Input 7 can additionally be used as potential free pulse counter input for odometer signals. Input 6 and 7 are referenced to GNDISO (isolated ground, X11 pin 3). An isolated 5 V power supply VISO is available at X11 pin 4. A Pull-up (to VISO 5 V) or a Pull-Down (to GNDISO) on IN7 is configurable by software.

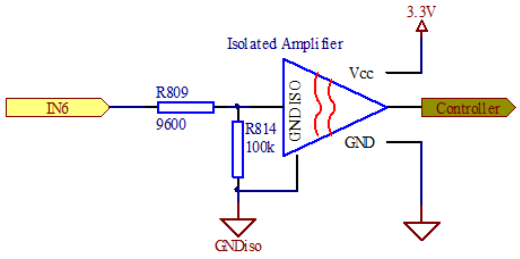


Figure 23: Principle of digital input 6

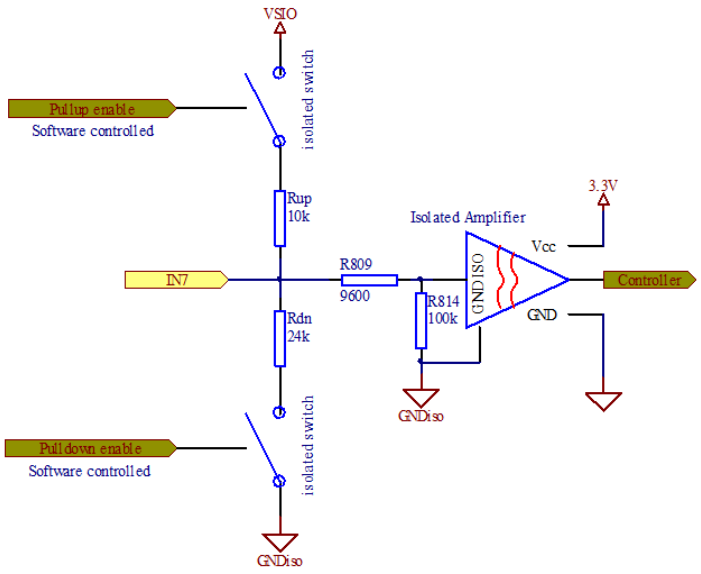


Figure 24: Principle of digital input 7

Digital input IN6 and IN7: Electrical Properties

Maximum input voltage (between IN6/IN7 and GNDISO)	50.4 V
Maximum reverse voltage (between IN6/IN7 and GNDISO)	-50.4 V
Isolation	+/- 500 V_{DC}
Minimum high level input voltage	4 V
Maximum low level input voltage	1 V
Input resistance	10 kOhm
Maximum switching frequency	IN6: 10 Hz IN7: 15 kHz

Table 17: Digital input IN6 and IN7: Electrical Properties

2.4.9.4 Digital Input 8

A digital input is available that is isolated from the internal circuitry with an opto-coupler. The principle of the input is shown in Figure 25 (protection diodes are not shown).

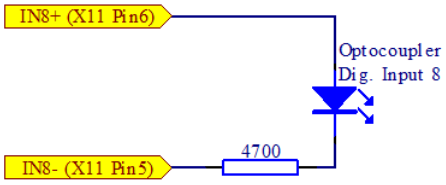


Figure 25: Principle of digital input 8

Digital Input 8: Electrical Properties

Maximum input voltage (between IN8+ and IN8-)	60 V
Maximum reverse voltage (between IN8+ and IN8-)	-60 V
Isolation	+/-500 V_{DC}
Minimum high level input voltage	10 V
Maximum low level input voltage	2.5 V
Input resistance	5 kOhm
Maximum switching frequency	10 Hz

Table 18: Digital Input 8: Electrical Properties

2.4.9.5 Wiring examples

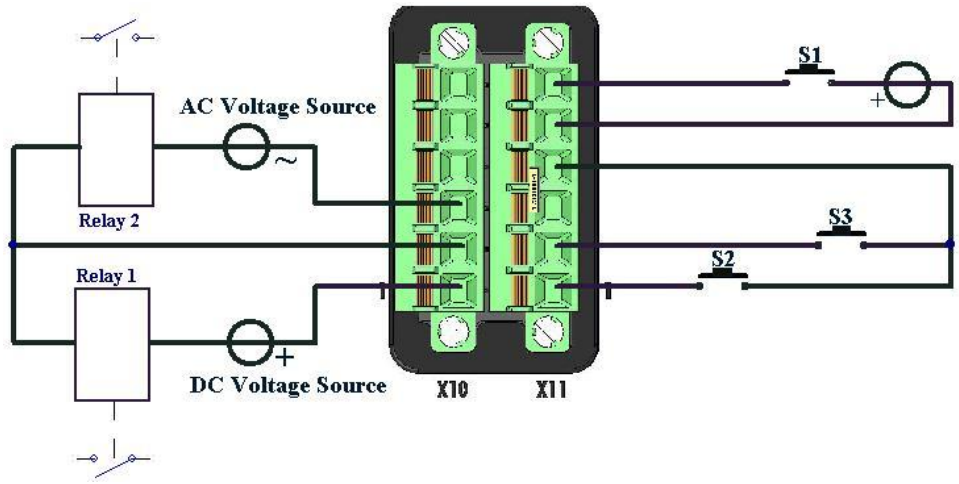


Figure 26 shows two relays connected to digital outputs 1 and 2, sharing a common current return.

IN8 is connected to a switched external voltage source. IN6 and IN7 are switched on/off via S2 and S3 using the internal isolated 5V supply.

Figure 26: Digital outputs and digital inputs 6, 7 and 8

Note: Relay 1 is a DC relay and relay 2 is an AC relay. Max. current 100 mA.

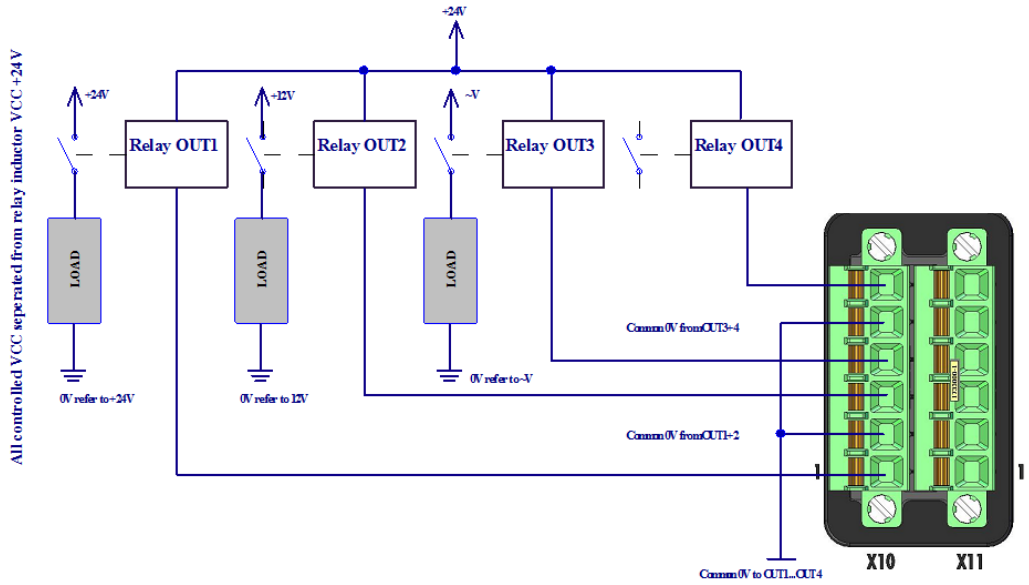


Figure 27 shows the wiring of digital outputs OUT1 … OUT4 for different power sources.

Figure 27: Digital outputs

2.4.10 Connector for accessory modules (X12, option)

Valid for:

☒ PCU-210 (G1)	☒ PCU-220 (G2)	☒ PCU-230 (G1)	☒ PCU-250 (G1)
☒ PCU-210 (G2)		☒ PCU-230 (G2)	☒ PCU-250 (G2)

See page 17 for information about the groups G1 and G2.

The interface is designed as DB9 male connector and reserved for accessory modules and optional functions (see chapter 2.5).

Note: X12 is not an RS-232 interface or similar standard interface! It is a specific interface which is used to connect the configuration plug SST-100 for example. Wiring can differ from model to model.

2.4.11 Status indicators (LEDs)

Valid for:
☒ PCU-210 (G1) ☒ PCU-220 (G2) ☒ PCU-230 (G1) ☒ PCU-250 (G1)
☒ PCU-210 (G2) ☒ PCU-230 (G2) ☒ PCU-250 (G2)

See page 17 for information about the groups G1 and G2.

	PCU-210		PCU-220	PCU-230		PCU-250	
	(G1)	(G2)	(G2)	(G1)	(G2)	(G1)	(G2)
Front LED indicators	ERR (R) PWR (G) ACT (G)	ERR (R) PWR (O) ACT (G) IN 1 (G) IN 2 (G) IN 3 (G) IN 4 (G)	ERR (R) PWR (O) ACT (G) IN 1 (G) IN 2 (G) IN 3 (G) IN 4 (G)	ERR (R) PWR (G) ACT (G)	ERR (R) PWR (O) ACT (G) IN 1 (G) IN 2 (G) IN 3 (G) IN 4 (G)	ERR (R) PWR (G) ACT (G)	ERR (R) PWR (O) ACT (G) IN 1 (G) IN 2 (G) IN 3 (G) IN 4 (G)
Rear LED indicators [1)]		PWR (O) ACT (G) USB (G)	PWR (O) ACT (G) USB (G)		PWR (O) ACT (G) USB (G)		PWR (O) ACT (G) USB (G)

Table 19: Overview of status indicators

(R) = red, (G) = green, (O) = orange

[1)] The rear LED indicators "PWR" and "ACT" are only available in the switch variant.

Power LED "PWR" (green or orange): Indicates that 16V...45V power is supplied to the PCU.

Error LED "ERR" (red): The red error LED "ERR" is active when the device is powered up and will remain active for a short period until the firmware has been bootstrapped.

An active LED "ERR" during operation indicates an error. Certain errors are associated with an error code. If such an error occurs, it is not only logged to the system log of the device but also displayed in the form of Morse code on the red error LED. The error code is repeated periodically. Please refer to the chapter 5.16 for a detailed description of error codes, possible causes and solutions.

Ethernet Activity LED "ACT" (green): Indicates if Ethernet is connected and if there is traffic:
off: No Ethernet link.
green: Ethernet link established.
blinks green: Ethernet traffic.

PCU-200 models with switch functionality and two Ethernet interfaces have an additional Ethernet activity LED "ACT" at the rear which indicates the status of the Ethernet interface X06 on the rear. The LED at the front indicates the Ethernet communication status of the Ethernet interface X04 on the front.

Input Activity LED indicators "IN1", "IN2", "IN3", "IN4" (green): Indicate an active opto coupler of the appropriate digital input (X02 pin 1-4). That means: current flows between the appropriate input pin and the common reference pin (X02 Pin 5).

2.5 Accessories

2.5.1 Configuration Plug SST-100 (X12, Option)

Valid for:

☒ PCU-210 (G1)	☐ PCU-220 (G2)	☐ PCU-230 (G1)	☒ PCU-250 (G1)
☒ PCU-210 (G2)		☐ PCU-230 (G2)	☒ PCU-250 (G2)

See page 17 for information about the groups G1 and G2.

The configuration plug SST-100 stores the configuration data of the PCU (see chapter 4.3). It is plugged in on the rear of a PCU via the D-SUB 9 connector (X12) and can be bolted there.

- No additional power supply necessary
- RoHS/CE, compatible for road and rail applications
- Flexible steel rope for permanent fastening at the place of installation inside the vehicle

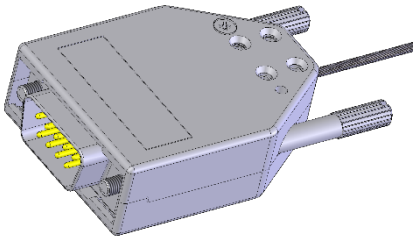


Figure 28: SST-100 configuration plug

Pin	Signal	I/O	Level
1	TWI-SCL	O	Clock signal for TWI
2	Reserve		
3	Reserve		
4	Reserve		
5	Reserve		
6	TWI-SDA	I/O	Data signal for TWI
7	3.3 V Input	PWR	3.3 V Input
8	GND	PWR	Signal GND
9	GND	PWR	Signal GND

Table 20: SST-100 connector pinning

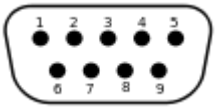


Figure 29: SST-100 connector

Note: X12 is not an RS-232 interface or similar standard interface! It is a specific interface which is used to connect the configuration plug SST-100 for example. Wiring can differ from model to model.

2.5.1.1 Dimensioned drawings SST-100

(All values in millimeter.)

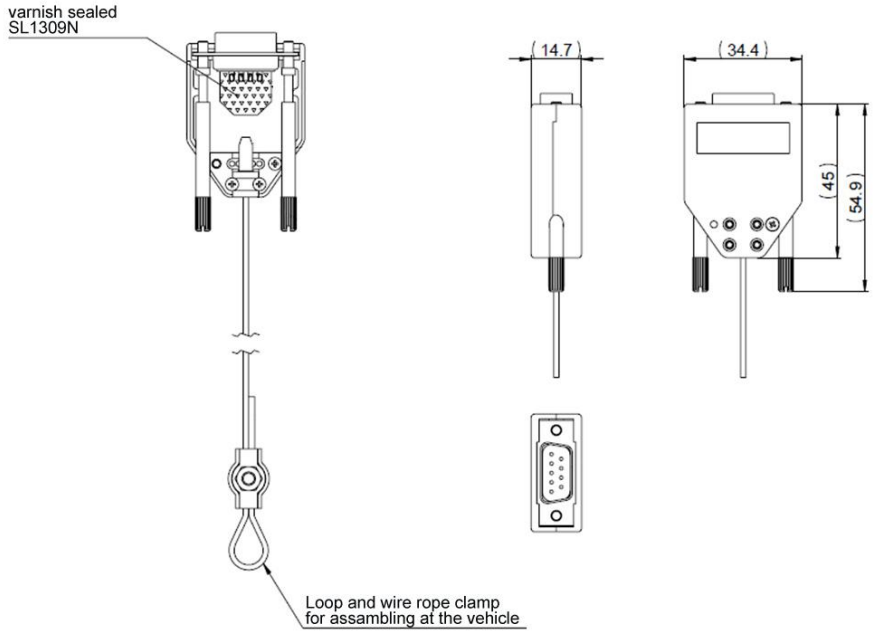


Figure 30: Dimensions SST-100

2.5.1.2 Mounting SST-100

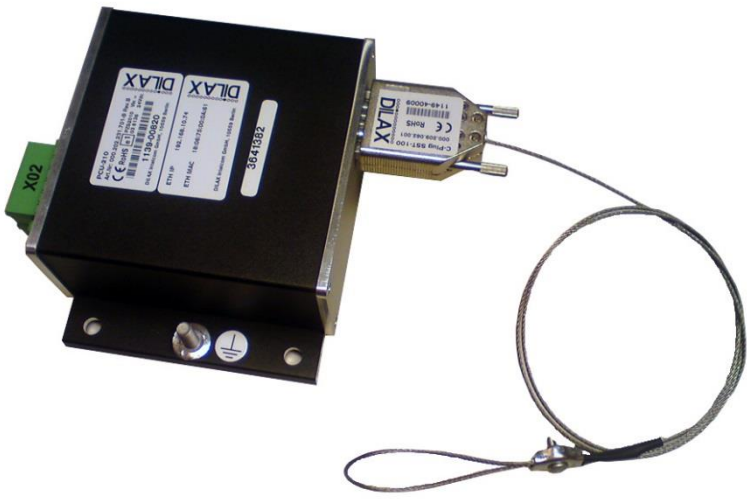


Figure 31: SST-100 mounting

After connecting the SST-100 to X12 tighten the bolts for mechanical protection.

To ensure the plug cannot be removed, fasten the steel rope directly at the vehicle.

2.5.1.3 Technical Data SST-100

Electrical Data

Nominal voltage	None
Current consumption @ 3.3 V	Max. 30 mA (depending on environment)

Table 21: Electrical data SST-100

Mechanical Data

Dimensions (L x W x H)	50 x 35 x 15 mm
Weight	90 g
Material	Metal

Table 22: Mechanical data SST-100

Environmental Data

Operating temperature	-25°C - +70°C
Storage temperature	-40°C - +70°C
Relative humidity	95 %
Protection class	IP40 (circuit board coated)
Shock and vibration	EN 61373 category 1, class B
EMC (tested with PCU-200 device)	EN 50155 / EN 50121
UL94 classification housing	Metal

Table 23: Environmental data SST-100

2.5.1.4 Trouble shooting SST-100

Problem	Possible reason	Correction
Data was not saved	Defect memory IC	Replace SST-100
	Not correct connected	Tighten the screws
	Bent D-SUB 9 pins	Bend pins to correct position
	Pin slid in into the D-SUB 9 connector	Replace SST-100

Table 24: Trouble shooting SST-100

2.5.1.5 Ordering Information SST-100

Article number	Description
000.209.062.001	SST-100 configuration plug

Table 25: Ordering information SST-100

2.5.2 Pull-down Resistor PDR-100

Valid for:

☒ PCU-210 (G1)	☒ PCU-220 (G2)	☒ PCU-230 (G1)	☒ PCU-250 (G1)
☒ PCU-210 (G2)		☒ PCU-230 (G2)	☒ PCU-250 (G2)

See page 17 for information about the groups G1 and G2.

The PDR-100 is a 19" rack plug in which allows an additional load resistance per input channel. The PDR-100 allows parallel connecting of resistors between input IN1...IN4 and a common reference potential INcom.

- No additional power supply necessary
- Simple cascading (serial)
- RoHS
- IK08

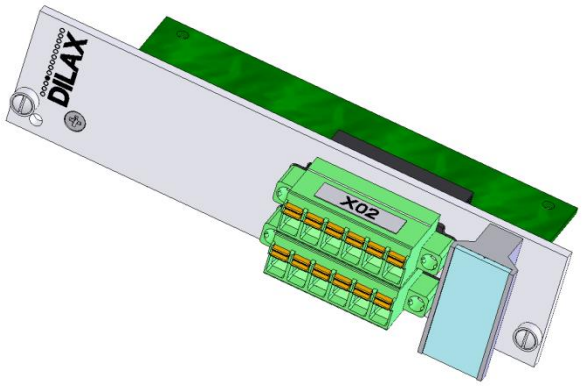


Figure 32: Pull-down resistor PDR-100

Row X01 of the Phoenix connector allows the connection to the PCU-200. Row X02 is for the connection to the local system. Every pin of the two rows is internally parallel connected.

X01 of the PDR-100			
Pin	**Signal**	**I/O**	**Level**
1	IN1	I	60 V_{DC}; connected to X02-1 of PCU
2	IN2	I	60 V_{DC}; connected to X02-2 of PCU
3	IN3	I	60 V_{DC}; connected to X02-3 of PCU
4	IN4	I	60 V_{DC}; connected to X02-4 of PCU
5	IN-Common	I	60 V_{DC}; connected to X02-5 of PCU
6	CASE		connected to X02-6 of PDR-100 and front panel

X02 of the PDR-100			
Pin	**Signal**	**I/O**	**Level**
1	IN1	I	60 V_{DC}; connected to X01-1 of PDR-100
2	IN2	I	60 V_{DC}; connected to X01-2 of PDR-100
3	IN3	I	60 V_{DC}; connected to X01-3 of PDR-100
4	IN4	I	60 V_{DC}; connected to X01-4 of PDR-100
5	IN-Common	I	60 V_{DC}; connected to X01-5 of PDR-100
6	CASE		connected to X01-6 of PDR-100 and front panel

Table 26: PDR-100 connector pinning

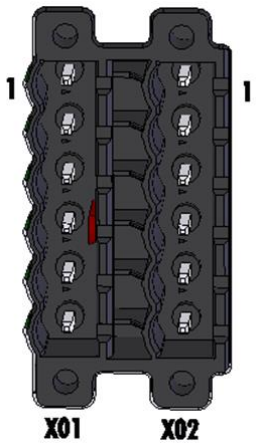


Figure 33: PDR-100 connector

2.5.2.1 Connection wiring and block diagram PDR-100

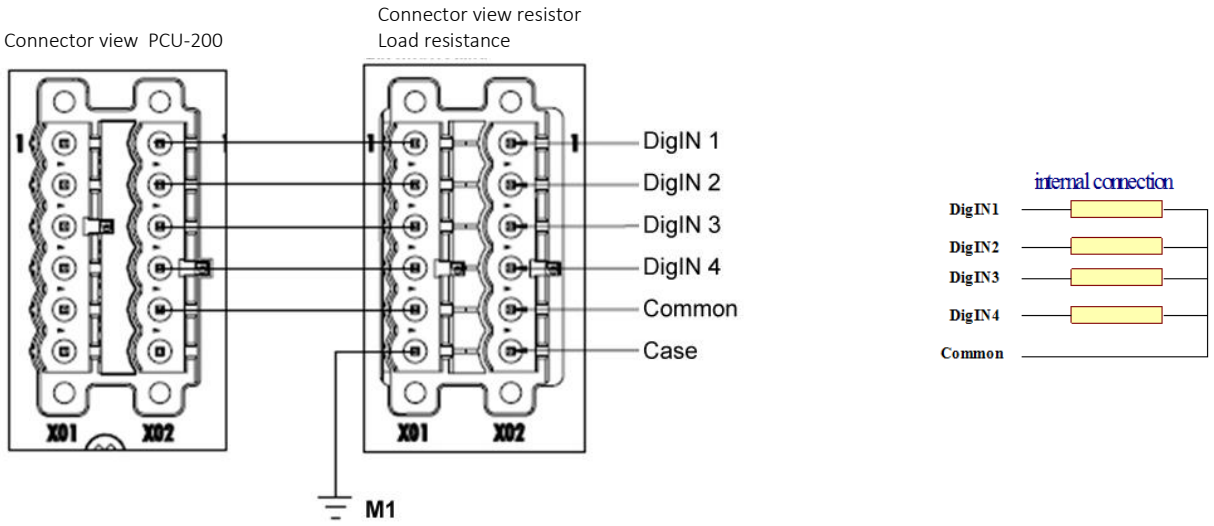


Figure 34: Connection wiring (left) and block diagram (right) PDR-100

The common input (pin 5 of X01 and X02) of the PDR-100 may be connected to GND or V_{CC}:

- When connected to GND: resistors are pull-down
- When connected to V_{CC}: resistors are pull-up

2.5.2.2 Mounting PDR-100

Mounting with connectors on the front

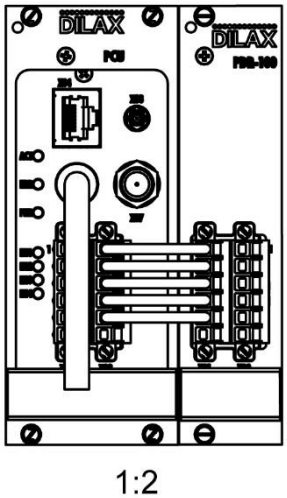


Figure 35: Mounting PDR-100

The pull-down resistor is pushed into a 19" rack and attached with 2 safety screws. The rack needs a width of 6 HP.

2.5.2.3 Dimensioned Drawings PDR-100

(All values in millimeter.)

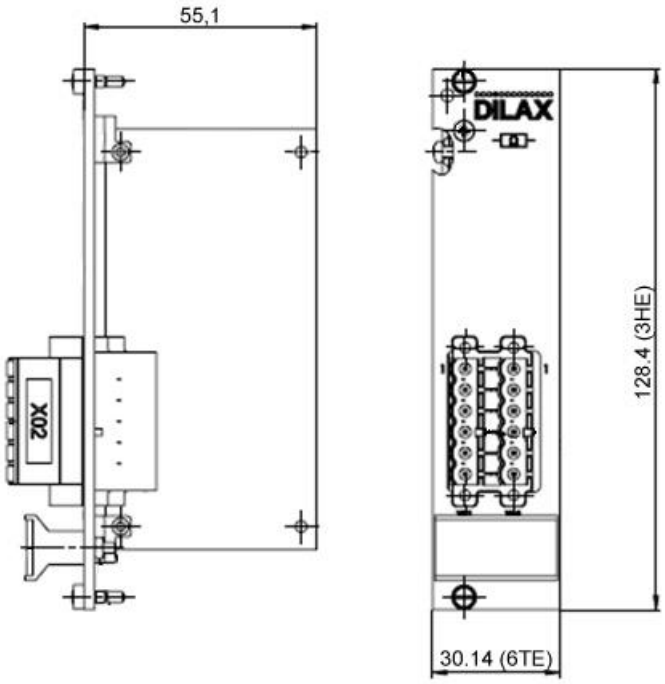


Figure 36: Dimensions PDR-100

2.5.2.4 Technical Data PDR-100

Electrical Data

Nominal voltage	None
Current consumption	Max. 60 mA per resistor @ 60 V_{in} (depending on environment)
4x single resistor	1 kOhm P ≥ 4 W

Table 27: Electrical data PDR-100

Mechanical Data

Dimensions (L x W x H)	130 x 56 x 30.4 mm
Weight	90 g

Table 28: Mechanical data PDR-100

Environmental

Operating temperature	-25°C - +70°C
Storage temperature	-40°C - +70°C
Relative humidity	95 %
Protection class	IP40 (circuit board coated)
Shock and vibration	EN 61373 category 1, class B
UL94 classification housing	V-0

Table 29: Environmental data PDR-100

2.5.2.5 Ordering Information PDR-100

Article number	Description
000.209.066.206	PDR-100

Table 30: Ordering information PDR-100

3 Configuration

A PCU is configured by a configuration file which can be modified via configuration pages of a web interface.

The status of a PCU can also be monitored via the configuration pages of the web interface:

- **Device Information:** Shows static information (e.g. serial number, article number, firmware version) and a live view of various data (e.g. WLAN, GPS, GSM, vehicle signal status) along with detailed counting data per door and per sensor. (See chapter 5.4.2)
- **Live Counting View:** Shows a live view of counting data per configured door. (See chapter 5.4.1)
- **Log Viewer:** Shows the current log messages. (See chapter 5.1)

3.1 Opening the Web Interface

The PCU-200 series provides a web interface for configuration, monitoring, and maintenance of the device. This interface can be accessed by a usual web browser. Supported are: Mozilla Firefox from version 3.5 onwards and Internet Explorer IE 8.0/9.0.

Note: JavaScript must be enabled in the browser.

To use Web Interface versions prior to 1.6.0 in Internet Explorer Version 9, you must perform the following steps in Internet Explorer 9: Press F12, and in the newly opened window change the "Browser Mode" from "IE9" to "IE8".

To access the web interface of the PCU, enter the IP address of the device directly into a web browser. Depending on the configuration, the IP address can be static or a dynamic:

- **The PCU uses a static IP address:**
  The IP address can be found on the identification plate/label of the PCU. The default IP address of a non-configured PCU is 192.168.23.200.
- **The PCU uses a dynamic IP address:**
  The IP address is dynamically assigned by a DHCP server. The assigned IP address must be known in order to access the web interface of the PCU.

Enter the PCU's IP address into the address bar of the web browser and confirm the entry to open the web interface.

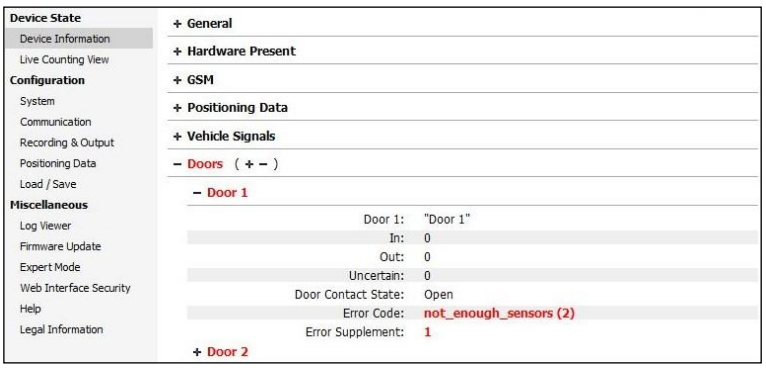


Figure 37: Web interface (example view)

When loading the web interface in the browser, it will contact the PCU device and load data such as the device information and configuration. You can view and modify this information, as described in the following sections. The language defined in the browser options[1] is selected as default. The language can be changed using the drop-down list

in the top right corner of the web interface.

Note: When changing the language, any unsaved changes will be lost. So it is strongly recommended to select the desired language of the web interface before setting any parameters.

3.2 Overview of the Operating Elements

On the left the web interface shows a menu with all functions. Click on a function to open it. If a PCU does not use a specific feature like GSM, GPS, or WLAN the corresponding configuration page will usually not be displayed in the menu.

Settings are usually defined with the following types of configuration elements. They can be operated in a manner that you are accustomed to from your operating system and browser.

Input fields: Example

Check boxes:

Drop-down lists: Example

Options:

Note: Detailed information about specific elements on the web interface
Many configuration elements have a help text on the web interface. Click on the "Help" icon, a blue question mark next to the configuration element, to display its detailed explanation.

Optional settings

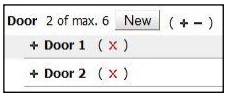
Some elements of the configuration are optional. Whether these optional elements are included in the configuration is controlled by a check box which is displayed next to or above the elements input field. Optional drop-down lists can be removed from the configuration by selecting the value **(not specified / default)**.

Operating elements in gray color

Input fields that are not allowed to be edited appear grayed out (displayed in gray color) and you cannot change its value. This happens when you decide not to include this element in the configuration.

Several identical configuration elements

Some configuration elements may appear several times (for example, there can be multiple doors). Such elements are shown one below the other and they can be expanded and collapsed. Additionally, there is a possibility to create a new element or to delete an existing element. When no item is shown, there are currently no existing configuration elements.



New Creates a new element (unless the maximum number of elements has been reached).

x Appears at every configured element. Click on it to delete the appropriate element.

Warning: Deleting an element cannot be undone.

Configuration elements with defined formats

Some configuration elements may only have specific formats (e.g. numbers in certain ranges, etc.). The input fields for such elements are labeled with information on the allowed formats. Such restrictions must be observed when entering values to avoid errors when saving the configuration.

Opening and closing areas

Some pages contain areas which can be opened and closed. Click on "+" left to the area name to open the area and click on "-" to close the area. An area name appearing in red letters points out an error. Open the area to get further information.

3.3 Password Protected Accessing the Web Interface

P.1. 1.10.5.1.4

The access to the web interface can be protected by a password. To setup a password open the page **Miscellaneous > Web Interface Security**.

Figure 38: Configuring a password to protect the web interface usage

Activate the check box **Web Interface Password Protection**. Enter the **New Password** and repeat it in the **New Password (Repeated)** input field. Press the **Save Security Settings** button to protect the web interface. The protection is applied immediately: After confirming the success message you will be asked to authenticate.

Figure 39: Authentication dialog box

Enter "admin" as **User Name** and your **Password**.

If you have lost the password, use the “daily password” to unlock the web interface (see chapter 5.3).

Note: Language of the authentication dialog box
The language of the authentication dialog box depends on the language settings of the operating system. Therefore it can differ from the language of the web interface.

Note: The authentication dialog box does not appear
The browser stores authentication data in cache storage. If the browser can authenticate the access to the web interface by using the cache data, no authentication dialog box will appear.

3.4 Saving the Configuration

Open the **Configuration > Load / Save** page.

Figure 40: Load / Save page

Note: Configuration changes must be saved and the device must be rebooted so that these changes become effective.

Click on the **Save Configuration to Device** button. If an error occurs while saving the configuration a corresponding error message will be shown. Such errors typically occur because of an invalid value in a field. The error message contains information on the affected field(s). If the configuration has been successfully saved a success message will be shown.

When the configuration has been saved successfully it is recommended to reboot the device to activate all changes. Press the **Reboot Device** button.

Figure 41: Reboot the device

3.5 Configuration > System > General

Use **Configuration > System > General** for configuring the general PCU device setup:

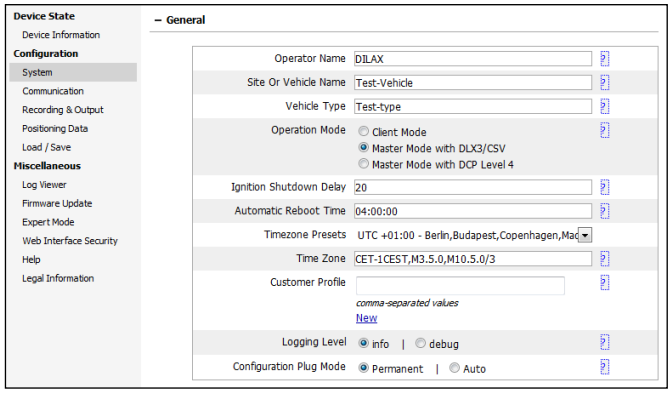


Figure 42: Configuration of general device settings

Identification and labeling

With this page you can define an **Operator Name**, a **Site Or Vehicle Name** and/or a **Vehicle Type** for identifying the counting data sets generated by this PCU.

Note: When you want to use the firmware update via FTP client function you need to configure the fields **Operator Name** and **Site Or Vehicle Name**. Consider the following rules:

- Special characters are not allowed in free configurable fields like **Operator Name**, **Site Or Vehicle Name**, **Vehicle Type**, **Door Identifier** etc.
- Only use alphanumeric values like "A,B,C…a,b,c" and numbers. Special characters like "/;*;+" etc. are not supported. Use underlines ("_") instead of space characters.

Note: If the live tracking diagnostics functionality should be used (Configuration > Recording & Output > Live Tracking, see 3.19), the **Vehicle Type** parameter must be configured. It must contain the vehicle number and the door numbers which should be handled and has the following structure: <vehicle number>_<door>_<door>

Example: **Vehicle Type** = 3_2_4

The PCU is located in vehicle 3 and handles doors 2 and 4. All doors to be added to the parameter must be separated by an underscore (_). The sequence of doors is conform to the sequence in the SSL bus chain. It begins on the left side with the first door next to the PCU and ends on the right side with the last door.

Operation Mode

Select an **Operation Mode** to decide in which mode the PCU device shall operate in the local network. The default setting is “Client Mode”.

The PCU offers two operations modes for **mobile systems**: **Master Mode with DLX3/CSV** and **Client Mode**. A PCU that operates in master mode will carry out passenger counting and data recording in files formatted in DLX3 or CSV. In client mode the PCU only operates as a pure counting device that saves passengers boarding and alighting.

For **non-mobile systems in fields of stationary counting**, the PCU operates in master mode and carries out people counting and data recording in files formatted in DCP Level 4.

A PCU can control up to 12 (G1) or 16 (G2) sensors (see also page 17). This allows monitoring of a limited number of doors or passages. The operation modes allow extending a counting system with several PCUs so that more doors/passages can be monitored.

A counting system with several PCUs consists of one master PCU and one or more client PCUs. All PCUs are connected together via Ethernet network. The master PCU collects all counting data of the client PCUs and adds this data to data recording. Depending on the system architecture the master PCU has an additional communication module like GSM or WLAN for data transfer.

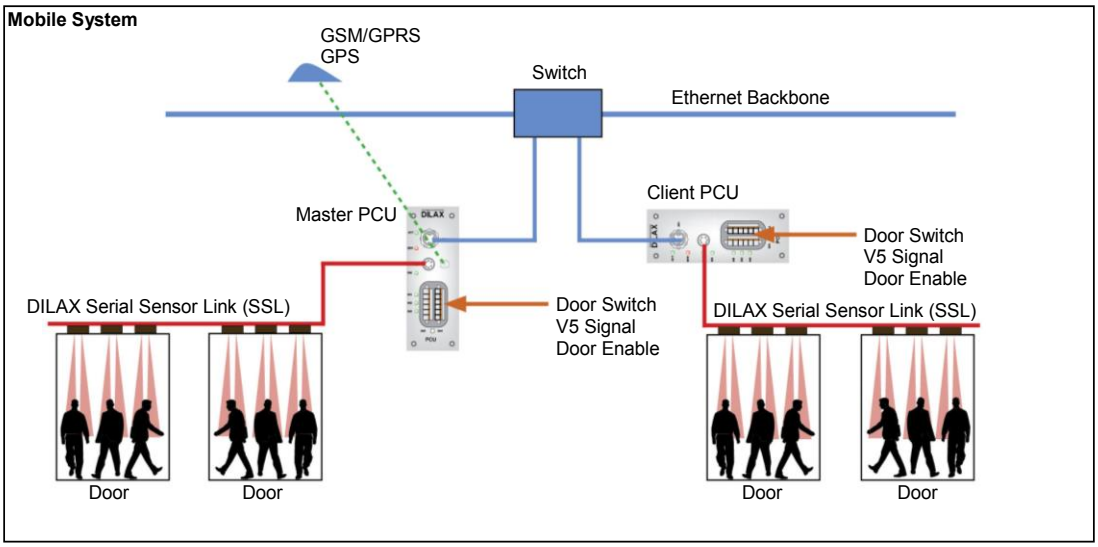


Figure 43: Master/client configuration of mobile systems

Ignition Shutdown Delay

This field defines the power down behavior of the PCU device, if there is an ignition or set up/out of operation signal connected to it. With this field, the PCU can be forced to shut down itself after a defined time delay. This ensures at final stops, that the last passenger movements can still be detected by the passenger counting system even though the vehicle's engine has been switched off. Please note that the door contacts also need to be configured correctly for this (see chapter 2.4.3.1).

Time for automatic reboot

In this field you can specify if and when the PCU is to restart automatically (reboot). An automatic restart is required in various applications in which the PCU is never shut down externally (continuous operation). This can be necessary for devices with a GSM module in particular, so that the PCU logs back in on the GSM network. For this purpose, the PCU can be configured so that it restarts automatically once per day. The time for the restart can be entered in the format HH:MM:SS. HH represents the hour of the day, MM the minute and SS the second. The seconds value is ignored and can even be left out, along with the preceding colon (HH:MM). The time entered must be the local time.

If the PCU is in operation and has a valid system time (after 1.1.2000 00:00:00) at the time configured for the automatic restart, it is restarted subject to a delay of one minute. Example: If a time of 01:00:30 has been configured, the PCU is restarted at 01:01:00. The seconds value is ignored. The PCU is restarted in the delay time between 1:01:00 and 01:02:00 and is no longer fully functional.

If this function is not to be used, the field remains empty.

Notes: Do not select a time range during clock change. This time range is skipped over or counted twice.

Time Zone

The PCU is equipped with an internal real-time clock (RTC) which is synchronized after system start with a valid time. Valid time data can be supplied by a navigation system (Navstar, Glonass), NTP server, IBIS system, or third-party system (via DCP and network interface) in the vehicle. Please note:

- The internal clock starts at 1970-01-01 00:00:00. Afterwards it is synchronized with the current time of the configured source.
- Synchronizing the system time can only be done via one source.
- Time data recording within data recording (DLX3 / live data / log files) is always done as Universal Time Coordinated (UTC) in UTC notation.
- The time zone is not considered in recorded data.

The configured time zone is used for calculating the local time. DLX3 data is transferred by using local time. At this time the recording file will be closed and transferred (file close time). Therefore, the PCU must be configured as master with DLX3/CSV recording. Example: UTC is 02:12:00 and the time zone is UTC +1. The resulting current local time is 03:12:00.

Choose the time zone to be used from the **Time Zone** selection list. Per default, no time zone is chosen: "(UTC)".

Notes: The time zones in the selection list become invalid when local time zone regulations change in the future. Current status: first quarter of 2013.

After updating or upgrading the firmware, the **Time Zone** setting must be checked and corrected, if necessary, and the configuration must be saved.

Customer Profile

Optionally, you can enter a customer profile. Enter all values separated by a comma. Alternatively, use **New** to enter each value into a separate input field. The complete profile is shown in the **Customer Profile** field.

Configuration Plug Mode

When the PCU supports the configuration plug SST-100 at the connector X12 (see chapter 2.5.1), the PCU can be configured to use the configuration plug in different ways (see chapter 4.3 for a detailed description):

- **Permanent mode:** The configuration plug is a fix part of the PCU and stores the configuration of the PCU. When the PCU is exchanged during a maintenance process, the configuration plug remains at the place of installation and must be connected to the new PCU.

Notes: The configuration is stored on both the configuration plug and the non-volatile memory of the PCU. If the configuration plug is not connected, the configuration cannot be stored on the configuration plug, a warning message appears and the configuration will be stored on the PCU.

If the configuration is not valid, an error message will be displayed and the configuration will not be stored on the configuration plug. The old configuration remains on the PCU and the plug.

If the configuration plug is unplugged after saving, the configuration remains on the PCU. If the configuration plug is plugged again, the PCU starts with the configuration from the configuration plug after next reboot (forced via web interface or normal boot up/shutdown procedure). The settings of the PCU will be overwritten!

- **Auto mode:** A master configuration is stored on the configuration plug to supply several PCUs with the same configuration. After electrical installation of the PCU, the configuration plug must be attached to the PCU. The master configuration will then automatically be copied from the configuration plug to the PCU's internal storage. When this process is finished, the PCU is configured with the master configuration and the configuration plug can be removed.

Notes: The configuration is stored on both the configuration plug and the non-volatile memory of the PCU. If the configuration of the PCU is changed via web interface, the configuration plug must be connected, otherwise an error message appears and the configuration will not be stored – neither in the PCU nor at the configuration plug. The old configuration remains on the PCU.

If the configuration is not valid, an error message will be displayed and the configuration will not be stored – neither in the PCU nor at the configuration plug. The old configuration remains on the PCU and the plug.

If the configuration plug is unplugged after saving, the configuration remains on the PCU. If the configuration plug is plugged again, the PCU restarts und uses the configuration from the configuration plug.

Do not confuse master configuration with configuration of a master PCU. A master configuration is stored at a configuration plug used to configure PCUs. The configuration of a master PCU is stored in the PCU which is configured in master mode.

3.6 Configuration > Communication > Network

Use **Configuration > Communication > Network** to configure the Ethernet network interface.

The PCU can be configured to get its IP configuration automatically from a DHCP server (see chapter 3.6.1), or you can define the IP configuration manually (see chapter 3.6.2).

3.6.1 Automatic IP configuration (DHCP)

Activate the check box **DHCP (Automatic)** so that the PCU will get its IP configuration automatically from a DHCP server as soon as it is connected to the network.

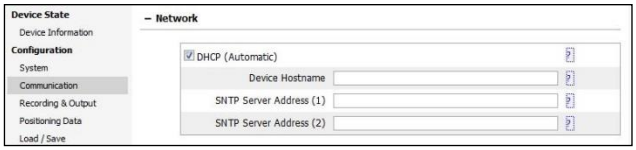


Figure 44: Configuration of the Ethernet network interface

In the **Device Hostname** input field you can define a hostname for the device. This is an optional input. It is used in the DHCP protocol to signalize the DHCP server which device is requesting an IP address.

The **SNTP Server Address (1)** input field allows configuring a time server for synchronizing the system time with a time reference (see chapter 4.1). This is an optional input. The time server delivers the current time to the PCU (UTC without considering time zones). It can be set automatically by the DHCP server or manually with this input field. For the time to be set automatically via the DHCP server, enter "auto" in this field.

Note: Some DHCP servers do not deliver the address of an SNTP server. In this case, enter the (S)NTP server manually even if all other IP settings are gathered automatically.

The IP address of a second SNTP server can be specified in the **SNTP Server Address (2)** field. If you specify a second SNTP server, an IP address must be specified in the **SNTP Server Address (1)** field as well. If two SNTP servers have been specified, the PCU determines the system time from the first SNTP server. If this server is not active (does not respond to time queries), the PCU uses the second SNTP server.

Note: If the address of the SNTP server is set automatically via DHCP, the keyword “auto” must be entered in the **SNTP Server Address (1)** field. The **SNTP Server Address (2)** field can be left blank. If the DHCP server supplies two SNTP server addresses, the address of the second SNTP server is also set automatically.

3.6.2 Manual IP configuration

If there is no (active) DHCP server in the network, you need to configure the IP configuration manually. To do this, deactivate the check box **DHCP (Automatic)** and insert the **IP Address** and **Subnet Mask** manually. Optionally, you can specify the IP address of the gateway, the first and the second DNS server.

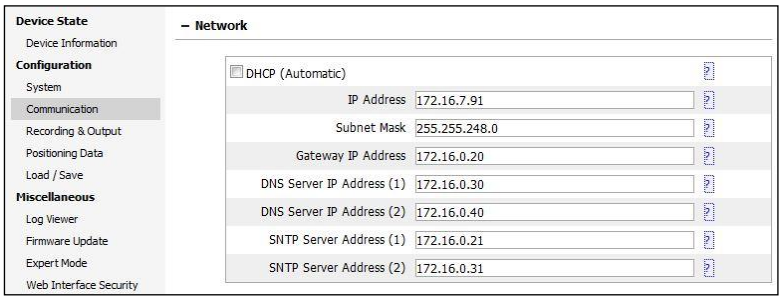


Figure 45: Manual IP configuration of the Ethernet network interface

Note: An IP address may not be assigned twice. Each PCU must have its own unique IP address.

You have to enter the **Gateway IP Address**, if the data transfer should be done by a third party system.

You have to enter at least one **DNS Server** when you want to use domain names instead of the dot-decimal-notation of IP addresses, for example for an FTP server, a time server etc. Please ask the on-site system administrator for detailed information.

A SNTP server to synchronise the system time can be used with a time reference in the **SNTP Server Address (1)** field (see chapter 4.1). The entry is optional. The SNTP server supplies the current time to the PCU (UTC without taking time zones into account).

The IP address of a second SNTP server can be specified in the **SNTP Server Address (2)** field. If you specify a second SNTP server, an IP address must be specified in the **SNTP Server Address (1)** field as well. If two SNTP servers have been specified, the PCU determines the system time from the first SNTP server. If this server is not active (does not respond to time queries), the PCU uses the second SNTP server.

3.7 Configuration > System > Doors

With **Configuration > System > Doors** you can configure the door setup. One door configuration contains several parameters like door identifier, door contact, sensor bar, and so on.

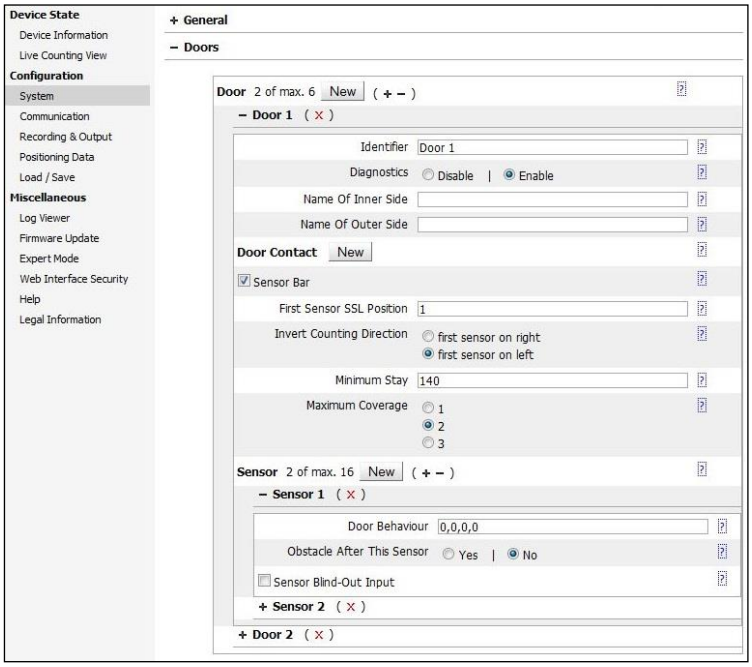


Figure 46: Configuration of the doors

Execute the following steps to create a setup profile for a door:

- Click on the button **New** next to **Door** to create a new door configuration profile.

Identifier

- Enter the name of the door. The identifier of every door shall be unique for the complete vehicle. Avoid using special characters (e.g. Ü, ä, *, or others). Use underlines instead of space characters.

Note: If the live tracking diagnostics functionality should be used (**Configuration > Recording & Output> Live Tracking**, see 3.19), the **Identifier** parameter must have the following structure: [<Door name Text>]<Door number>. <Door name Text> as an option.

Example:
Identifier = door2
Vehicle Type = 3_2_4 (configured at **Configuration > System > General**)

The value of the **Identifier** parameter can start with a text (not numeric) and has to end with the door number.

For the **Vehicle Type** parameter only the door number is used.

Diagnostics

- If you want to record diagnostic messages of the door in the data record file enable **Diagnostics** (see chapter 5.5).

Notes:

The diagnostic function has to be deactivated for inner doors which are always open.

If **Diagnostics** are enabled, the PCU tests the plausibility of the door signals and the long term functionality of the sensors and generates diagnostic messages. This is done in addition to the error state detection of the doors.

Name Of Inner Side / Name Of Outer Side

- With these fields, the designations of the door sides are defined. These definitions are optional and have no effect on recorded data.

Door Contacts

Note: All doors at which people enter and leave a vehicle, must be correctly configured so that the whole counting system works error-free and has an optimal counting quality. Wrong or missing door configurations distort the counting results and therefore have a negative influence to the system's counting quality.

Counting sensors are always active and deliver data via the SSL bus. Sensor data is processed by the PCU under consideration of the configuration and counting results are determined. The PCU registers a counting object **when all of the following conditions are fulfilled**:

- The vehicle is not moving (velocity is max. 3 km/h or the appropriate signal is available at the digital input).
- At least one door is open or released (determination via configured signals at the digital inputs or network inputs).
- At least one object passes the counting sensor at the open door and remains for a defined minimum time (**Minimum Stay**) within the detection area. The minimum stay time for a door can be configured on the web interface.

Recommendation: The door signals should be configured to have 24 V_{DC} (active, high level) at the digital inputs of the PCU when the doors are closed, and 0 V_{DC} (inactive, low level) when the doors are open. This ensures that entering and leaving passengers are still counted even if the vehicle is standing still with switched off ignition (e.g. at final stops).

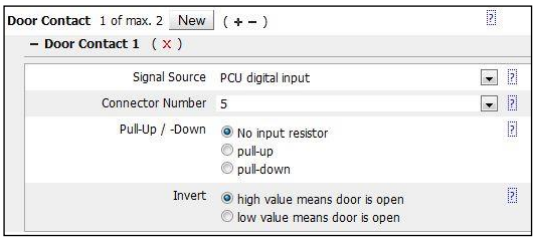


Figure 47: Configuration of the door contacts

For configuring a door contact execute the following steps:

- If the door has a door contact, create a new contact by clicking the button **New**. Further configuration options of the door contact will be displayed.
- Define the input source:
  - Choose the **Signal Source** of the contact, e.g. "PCU digital input", "network input" or "INP-450".
  - Depending on the chosen signal source, one of the following parameters must be defined:
    - **Connector Number** (this is the input number IN**x** and not the PIN number Xnn)
    - **Input Number** and **SSL Position** (INP-450 only)

Note: Each input source can only be chosen once. When defining several door contacts, choose a different combination of **Signal Source** and **Connector Number**, **Input Number**, or **SSL Position** for each configured door contact.

- If necessary, set a resistor option **Pull-Up / -Down**. This entry is related to the digital inputs IN5 (X02-6, see chapter 2.4.3) or IN7 (X11-2, only PCU-220 and PCU-250, see chapter 2.4.9).
- Set the **Invert** behavior.
  (default: high value means door is open)

Sensor Bar

In the **Sensor Bar** area you can configure the sensors located above the door.

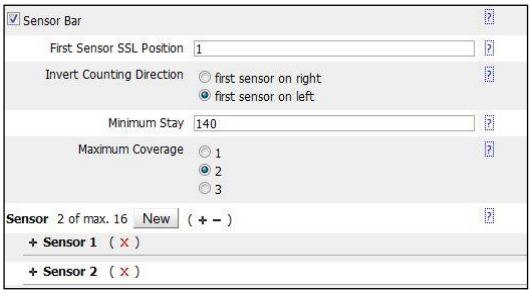


Figure 48: Configuration of the sensor bar

- Activate the check box **Sensor Bar** to define the available sensors of the door.
- Enter the position of the first sensor (starting at the PCU) within the whole SSL chain in the field **First Sensor SSL Position**.

  The SSL position describes the position of the sensor within the SSL chain starting at the PCU. Therefore, all SSL elements, incl. digital inputs, are to be considered.

- Look at the sensor bar from inside of the door. Choose the location of the first sensor at **Invert Counting Direction** as described below:

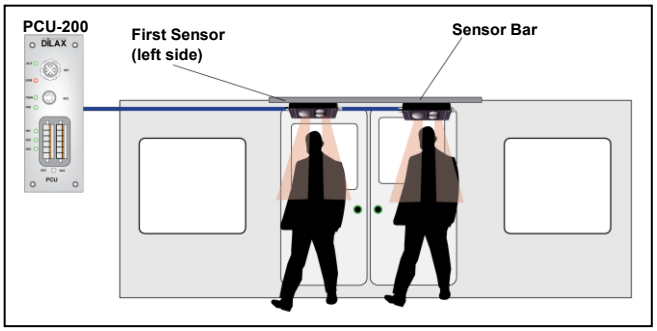


Figure 49: First sensor left

Select “first sensor on left” if the sensors are installed as shown in this figure.

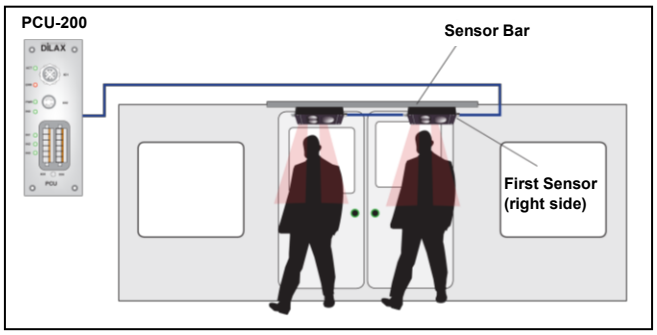


Figure 50: First sensor right

Select “first sensor on right” if the sensors are installed as shown in this figure.

- Set the **Minimum Stay** time (0...1000 milliseconds, default value: 140 ms). The minimum stay time is the time an object must dwell below the sensor to be registered as counting event.
  - Set the **Maximum Coverage** (values 1...3 in version 1.7.0 and higher; values 1...2 in older versions). When a person is passing a door, several sensors may register a counting event at the same time. To avoid double counting, adjacent sensors can be grouped by the maximum coverage function to build a logical sensor. All possible combinations of adjacent sensors are considered, see Figure 56.

    This mechanism in only active when a counting object is passing the sensors in one direction (e.g. IN). When objects are passing adjacent sensors in different directions (e.g. IN and OUT), maximum coverage has no effect.

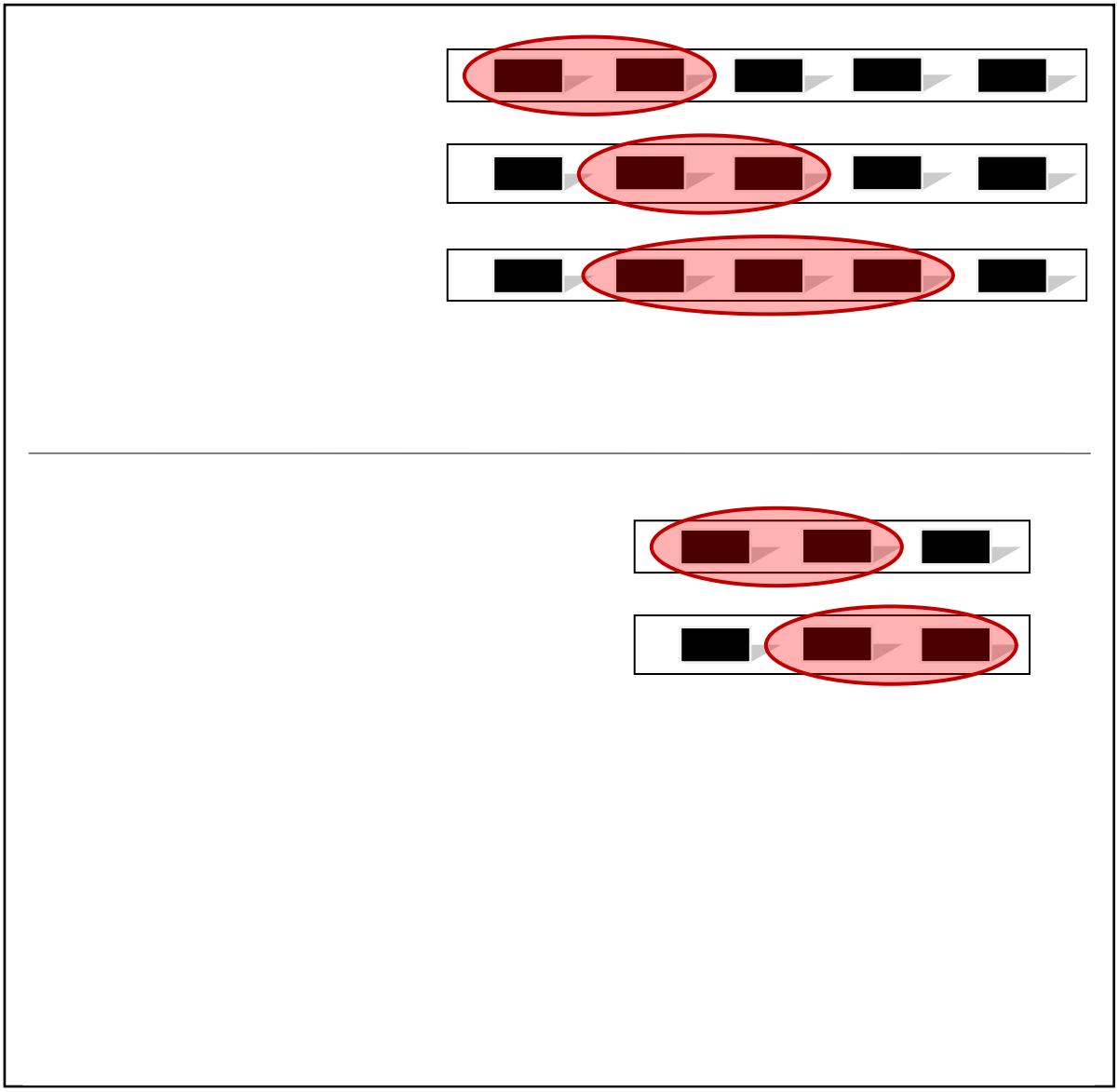


Figure 51: Examples for maximum coverage

Note: Special cases are doors which are divided into several passages. For these, the parameter **Obstacle After This Sensor** MUST be configured in addition. As a result, the passage is automatically divided into two areas and the functioning of the logical sensor is influenced so that the two areas are processed individually. Wrongly configured obstacles influence the counting results and therefore the counting quality of the system.

Sensor of a Sensor Bar

Mostly a sensor bar consists of several sensors. All sensors must be defined.

Note: Former revisions of the PCU hardware (G1) support a maximum of 12 sensors (see chapter 1.2). For these devices, if you try to save a configuration with more than 12 sensors an error message will be shown.

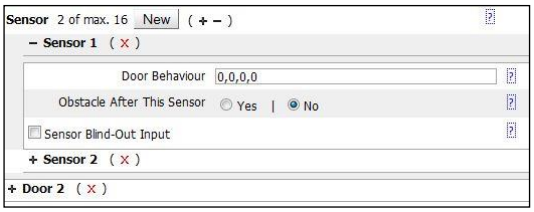


Figure 52: Configuration of a sensor of a sensor bar

- For each **Sensor** of the sensor bar you have to click the **New** button.
- With the **Door Behavior** parameter, the PCU's counting behavior for specific door types can be influenced. Let this field empty to use the default behavior.
- If there is an obstacle at a door between the sensors (needle separation, handrail, etc.), activate the check box **Obstacle After This Sensor** of the appropriate sensor.

Note: This setting is especially necessary in combination with the **Maximum Coverage** parameter which combines several sensors of the door to a logical sensor. The logical sensor will be divided into two logical sensors where the obstacle is defined.

A wrong configuration influences the counting results and the system's counting quality.

Please also note the installation instructions for the sensors in the corresponding sensor manual!

Sensor Blind-Out Input of a Sensor Bar's Sensor

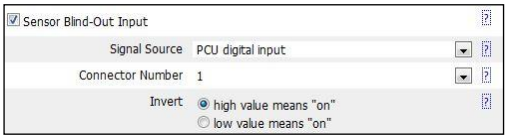


Figure 53: Configuration of the sensor blind-out input

- If there is a sensor blind out signal available for a sensor (to suppress counting of moving parts of the door) activate the check box **Sensor Blind-Out Input**. Further configuration options will be displayed.

- Define the input source:
  - Choose the **Signal Source** of the sensor blind-out input, e.g. "PCU digital input", "network input", or "INP-450".
  - Depending on the chosen **Signal Source**, one of the following parameters must be defined:
    - **Connector Number** (this is the input number IN**x** and not the PIN number Xnn)
    - **Input Number** and **SSL Position** (INP-450 only)

Note: Each input source can only be chosen once. When defining several sensor blind-out inputs, choose a different combination of **Signal Source** and **Connector Number**, **Input Number**, or **SSL Position** for each configured sensor blind-out input.

- If necessary, set a resistor option **Pull-Up / -Down**. This entry is related to the digital inputs IN5 (X02-6, see chapter 2.4.3) or IN7 (X11-2, only PCU-220 and PCU-250, see chapter 2.4.9). For all other inputs the selection of this entry will be ignored.
- Set input **Invert** behavior.
  (default: high value means "on" = not inverted)

If you have completed the configuration for a door, you can create an additional door profile by clicking the button **New** next to **Door** (see Figure 51).

3.8 Configuration > System > Rooms

This function allows calculating the current load of a complete vehicle (whole room) and of single rooms of a vehicle consist (single room). This allows, for example, analyzing the current load in different areas of vehicles or vehicle consists (first and second class, passage areas, luggage compartments, etc.).

The load is calculated by considering the counting values (difference between boarding and alighting passengers) and the configured maximum load capacity of the vehicle or the single rooms of the vehicle. It is displayed as a percentage in steps of 10 % for the whole room or single rooms of the vehicle. A load of < 10 % means: the current load is less than 10 % of the configured maximum load of the vehicle or room. A load of 100 % means: the configured maximum load of the vehicle or room is reached or exceeded. The calculation is done automatically and continuously in the background.

Note: To prevent a counting error continues for the whole journey, an error correction has been integrated. It works as follows:

When the value of the automatic load calculation is below 10%, further alightings are no longer considered; only boardings are considered. When the value is at least 100%, automatic load calculation does not consider further boardings, it considers only alightings. **The PCU's counting function is not influenced by this correction, it continues counting all recognized boarding and alighting passengers.**

Mandatory requirements for correct load calculation:

Vehicles must be equipped with counting sensors at correct positions in the vehicle AND the sensors must have been correctly installed according to the installation instructions.

Correct configuration of the rooms and the maximum load capacity. For a correct calculation, the whole vehicle or the whole vehicle consist must form a complete and closed whole room. This whole room may thereby be divided in several single rooms but there must be doors equipped with counting sensors between all single rooms.

Notes:

The outer doors are used to calculate the load of the whole room (complete vehicle area).

The inner doors are used in addition to calculate the load of single rooms.

The calculation of the whole load and the calculation of the load of single rooms are executed independently. Under unfavorable conditions, the whole load is not identical to the total load of the single rooms.

Load calculation is only possible for defined vehicle compositions. Load calculation cannot be used for dynamic vehicle compositions.

Load calculation data is transferred via the DILAX realtime protocol (DCP Level 3, live and station tracking). There is no recording of load values in the DLX3 archive.

Examples for correct room definitions: There is a complete and closed whole room.

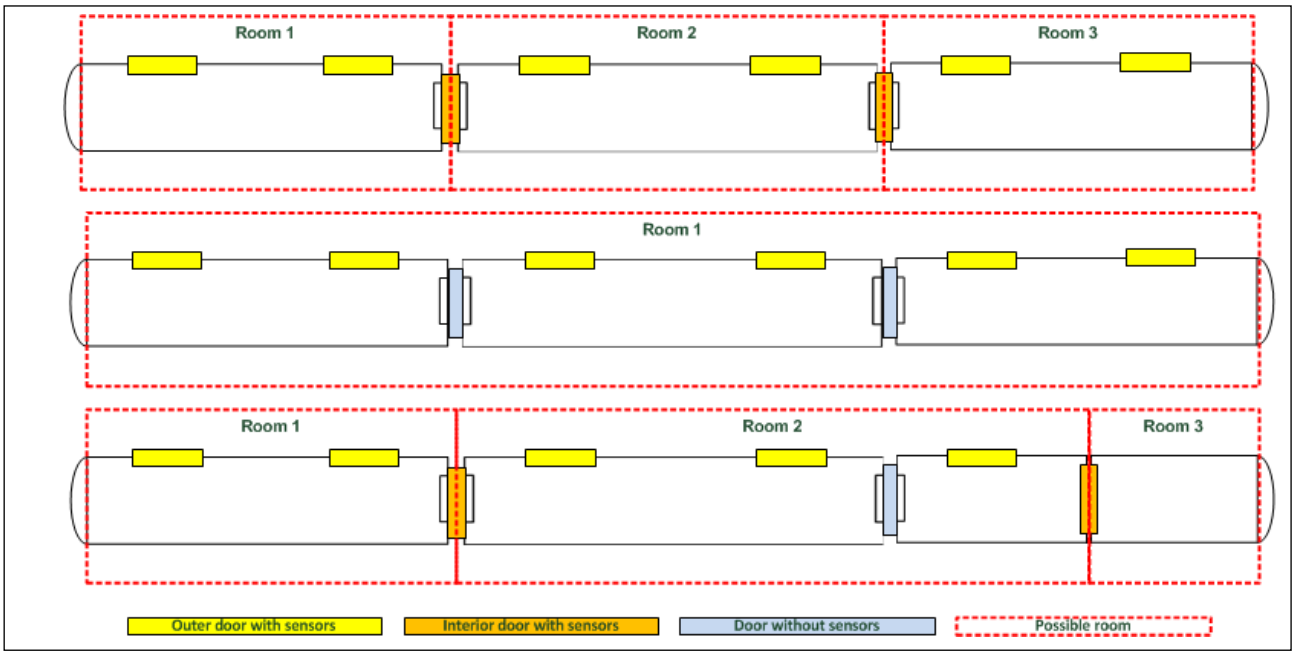


Figure 54: Examples for correct room definitions

1: The vehicle consist is split in three single rooms. For each wagon a single room has been defined. The inner single room is clearly separated from the outer wagons by interior doors with sensors. The whole room is completely defined and closed. The load of three single rooms will be calculated.

2: The vehicle consist is defined as one room. Single rooms cannot be defined because the interior doors between the wagons are not equipped with sensors. The whole room is completely defined and closed. The total load of the vehicle consist will be calculated.

3: The vehicle consist is split in three single rooms. The single rooms span several wagons. The middle single room spans two wagons and is separated from the right room within the right wagon by an interior door with sensors. The interior door between the middle and the right wagon is not equipped with sensors and can thereby not be used as room separator. The whole room is completely defined and closed. The load of three single rooms will be calculated.

Examples for wrong room definitions: The load cannot be calculated correctly because the whole vehicle consist is not completely split in single rooms.

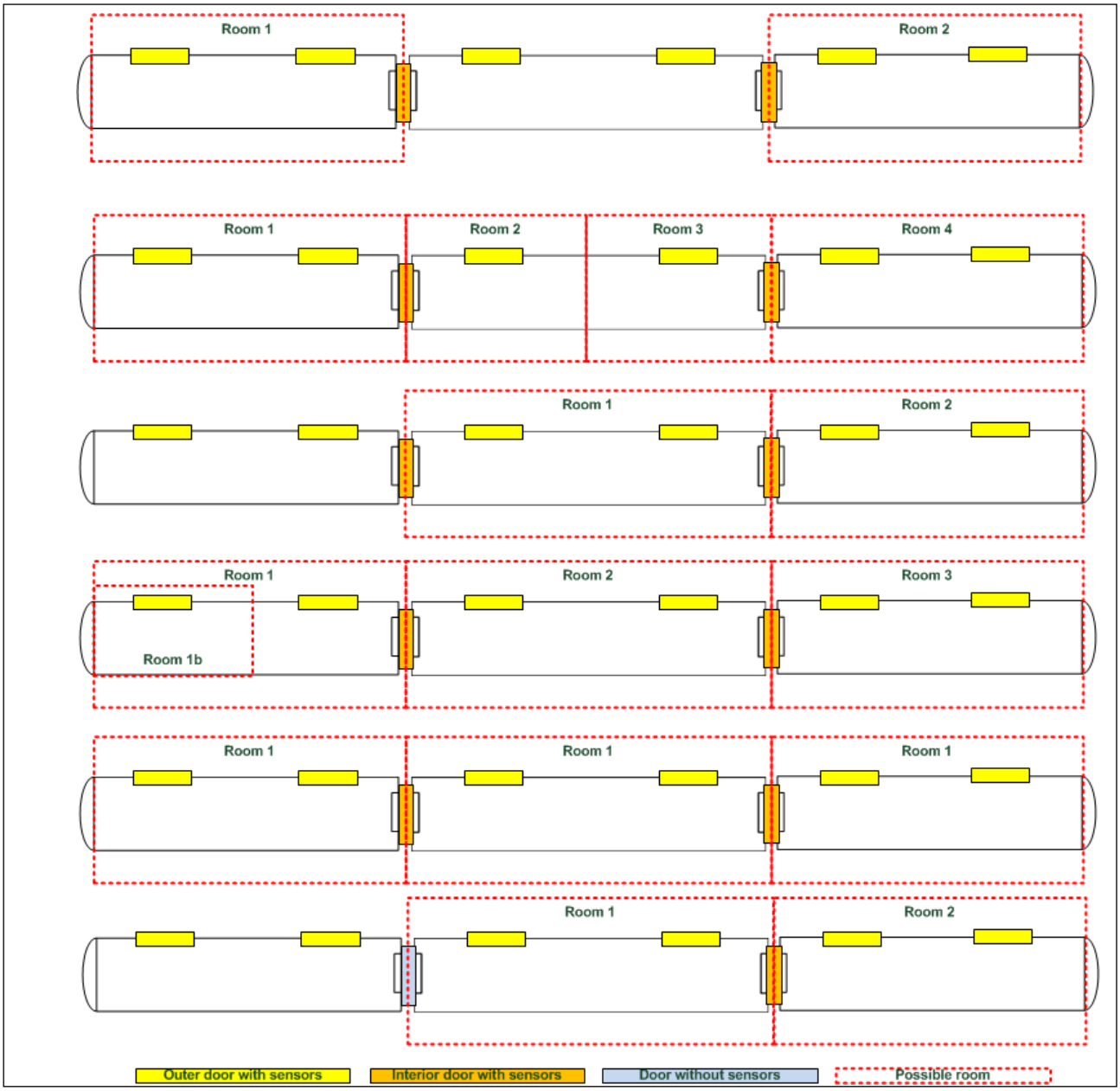


Figure 55: Examples for wrong room definitions

1: The vehicle consist is not completely split in single rooms. The middle single room has not been defined. The middle wagon has to be defined as single room bordered by outer and inner doors.
2: The vehicle consist is completely split in single rooms but the single rooms are not correctly defined. There is no interior door with sensors in the middle wagon between room 2 and room 3. The middle wagon has to be defined as one single room.
3: The vehicle consist is not completely split in single rooms. The left single room has not been defined. The left room has to be defined as single room bordered by outer and inner doors.
4: The vehicle consist is completely split in single rooms but room 1b is not clearly split from room 1 by an interior door with sensors. Room 1b has to be deleted from the configuration.
5: The vehicle consist is completely split in single rooms but the room names are not unique. Each single room has to get a unique name.
6: The vehicle consist is not completely split in single rooms. The interior door between the left and the middle wagon is not equipped with sensors. Room 1 has to span both, the left and the middle wagon.

Configuring rooms

Attention: Master mode with DLX3/CSV must be selected as **Operation Mode** in **Configuration > System > General** in order to configure rooms.

Wrong room definitions lead to wrong calculation of load values. Ensure that:

- the whole vehicle/vehicle consist is split in defined rooms.
- each room is clearly bordered by doors/interior doors with sensors
- each room has a unique name
- rooms bordered by a door are unique and correctly defined in the door definition (**Configuration > System > Doors**)

Proceed as follows to configure rooms:

Create a vehicle plan and define the splitting in rooms.

Define all doors (**Configuration > System > Doors**), the doors of the client PCU(s) as well as the doors of the master PCU.

The best way is to start with the last client PCU and to end with the configuration of the master PCU. Define the respective door sides and assign the room names which are necessary in step 3 to create room definitions in the master PCU. Save the configurations to the client PCUs and restart the devices so that all settings become operative.

In the door configuration, the input fields **Name Of Inner Side** and **Name Of Outer Side** are used to define the names for the door (see chapter 3.7). A passenger is on the outer side of a door when he went through the door and was counted as outgoing. Analogue, a passenger is on the inner side of a door when he went through the door and was counted as incoming.

Rooms and doors are interconnected by names. Therefore, the names of the sites of the door are marked with appropriate room names.

Interior door: the name of the room which borders to the outside of the door must be entered into the **Name Of Outer Side** field. The name of the room which borders to the inner side of the door must be entered into the **Name Of Inner Side** field.

Outer door: The name of the room into which the door leads must be entered into the **Name Of Inner Door** field. The **Name Of Outer Door** field remains empty.

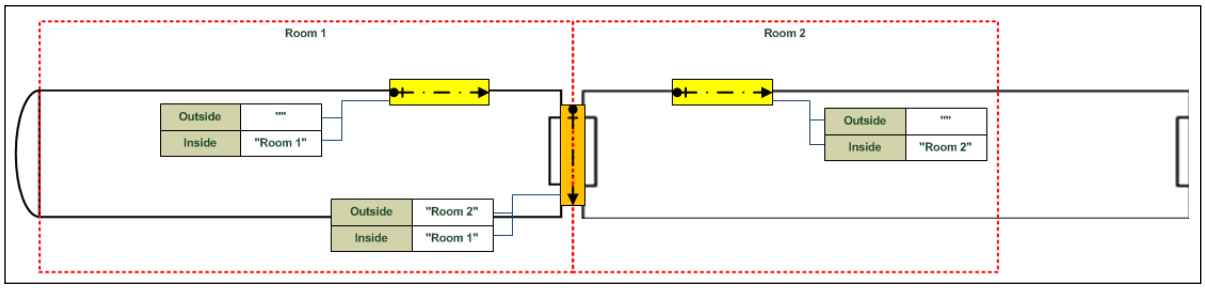


Figure 56: Names for inner and outer side of doors when having two rooms, an interior door and two outer doors

Define the rooms on the master PCU.

Rooms can only be configured on the master PCU. Use the room names which have been configured in step 2.

– Choose **Configuration > System > Rooms**.

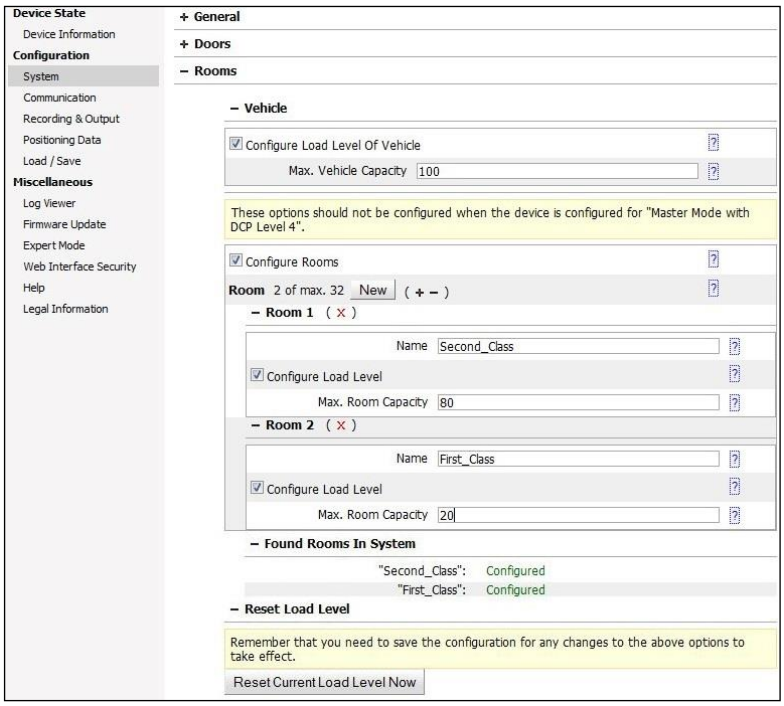


Figure 57: Configuration of rooms

- Activate and configure the load calculation of the whole vehicle/vehicle consist.

    1. Activate the **Configure Load Level Of Vehicle** check box. This activates the load calculation of the whole vehicle. The counting values of all sensors located at the outer doors are taken into account. This calculation is independent of the load calculation for rooms.

    2. Enter the maximum allowed number of passengers the vehicle or vehicle consist can carry into the **Max. Vehicle Capacity** field. This value is taken into account when the load of the whole room is calculated.

- Configure the single rooms of the vehicle/vehicle consist and activate the load calculation of these single rooms.

    1. Activate the **Configure Rooms** check box.

    2. Click on the **New** button to the right of **Room** to create a new room configuration profile. A maximum of 32 rooms can be defined.

    3. Enter the name of the room into the **Name** input field. Only letters and numbers are allowed to be used. Avoid special characters (ä, Ü, *, etc.). Use underlines instead of blank characters. The name must be unique for the whole vehicle/the whole vehicle consist.

    4. Activate the **Configure Load Level** check box and define the load calculation of the room in the vehicle.

    5. Enter the maximum allowed number of passengers the room can carry into the **Max. Room Capacity** input field. This value is taken into account when the load of the single room is calculated.

- Create further room configuration profiles. Also use the **Found Rooms In System** list.

    To simplify the configuration, the master PCU shows all room names which have been defined in the door configuration on the client PCUs in the **Found Rooms In System** list. A room is marked as "configured" when it is already defined in the **Configure Rooms** section on the master PCU. Among other things, use this list to check if your room configuration is complete.

Note: A room is marked as "configured" only then, when its room configuration is stored on the master PCU.

Rooms are only configured on the master PCU whereas the assignment of doors and rooms is done in the door configuration on the appropriate client PCU.

Resetting the current load level calculation

The calculation starts when the master PCU starts working (on power-on or after a manual reset). If necessary, the calculation can manually be restarted to set the difference between boarding and alighting passengers to 0 (zero). Therefore click on the **Reset Current Load Level Now** button.

Notes: As soon as a counting error occurs, the load level will be marked as erroneous. Resetting the load level also clears this mark.

The load level calculation will automatically be reset when the vehicle becomes operational, or when the configuration is stored on the master PCU by using the web interface.

3.9 Configuration > System > Vehicle Signals

The PCU-200 series supports different types of vehicle signals which can be configured in **Configuration > System > Vehicle Signals**.

Note: Do not use this menu to configure digital inputs which are defined as door contact. Use **Configuration > System > Doors** instead.

If you want to record diagnostic messages from vehicle signal monitoring enable **Diagnostics** (see chapter 5.5).

Definition of Common Input Types

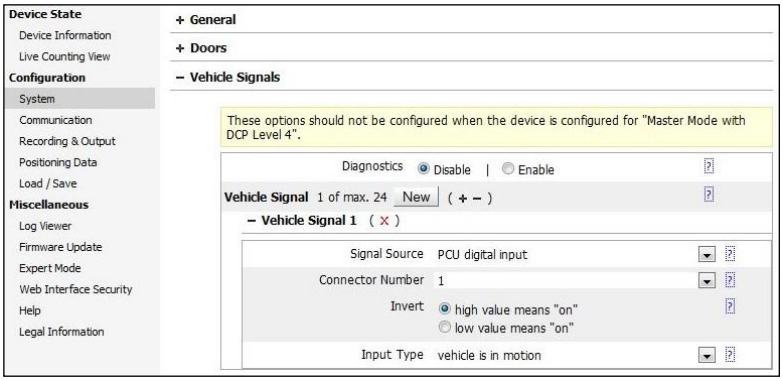


Figure 58: Configuration of common input types

Common input types are:

- vehicle is in motion
- door release, left side
- door release, right side
- vehicle operational
- vehicle at regular stop

- Click on the button **New** to create a new **Vehicle Signal**.
- Define the input source:
  - Choose the **Signal Source** of the vehicle signal, e.g. "PCU digital input", "network input", or "INP-450".
  - Depending on the chosen **Signal Source**, one of the following parameters must be defined:
    - **Connector** Number (this is the input number IN**x** and not the PIN number Xnn)
    - **Input Number** and **SSL Position** (INP-450 only)

Note: Each input source can only be chosen once. When defining several vehicle signals, choose a different combination of **Signal Source** and **Connector Number**, **Input Number**, or **SSL Position** for each configured vehicle signal.

- Select the vehicle signal connected to the digital input in the list **Input Type**.
- If necessary, set resistor **Pull-Up / -Down**. This entry is related to the digital inputs IN5 (X02-6, see chapter 2.4.3) or IN7 (X11-2, only PCU-220 and PCU-250, see chapter 2.4.9).
- Set the **Invert** behavior (default: high value means "on" = not inverted).

Definition of Input Type Odometer Input

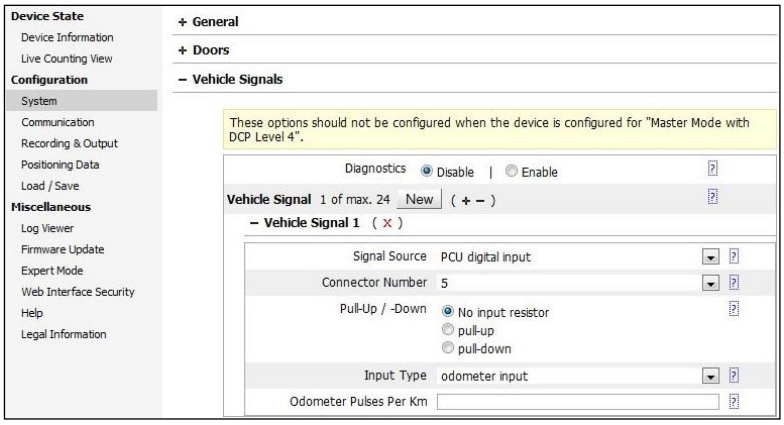


Figure 59: Configuration of the odometer input

1. Click on the button **New** to create a new **Vehicle Signal**.
2. Choose the **Signal Source**, e.g. "PCU digital input" for a physical input directly connected to the PCU.
3. Select the **Connector Number** 5 or 7 (see chapter 2.4.3.3 for wiring examples).

4. Select the **Input Type** "odometer input".

If known enter the **Odometer Pulses Per Km**. Otherwise enter "auto" which enables the automatic calibration of the odometer input by comparison of the pulses with the velocity measured by the GPS recording.

Note: The automatic calibration of the odometer input requires a device with GPS receive enabled, a vehicle in motion and GPS reception. The calibration is repeated at least at every system start of the PCU. Whenever possible, enter a concrete value at **Odometer Pulses Per Km**.

If necessary, set resistor **Pull-Up / -Down**. This entry is related to the digital inputs IN5 (X02-6, see chapter 2.4.3) or IN7 (X11-2, only PCU-220 and PCU-250, see chapter 2.4.9).

Definition of Input Type Event

The PCU can be configured to raise events when the states of digital inputs change.

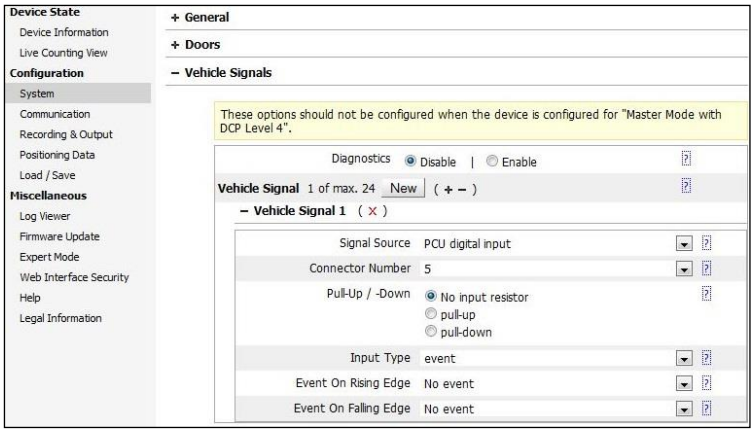


Figure 60: Configuration of an event generation

1. Click on the button **New** to create a new **Vehicle Signal**.
2. Define the input source:
   - Choose the **Signal Source** of the vehicle signal, e.g. "PCU digital input", "network input", or "INP-450".

- Depending on the chosen **Signal Source**, one of the following parameters must be defined:
  - **Connector Number** (this is the input number IN**x** and not the PIN number Xnn)
  - **Input Number** and **SSL Position** (INP-450 only)

Note: Each input source can only be chosen once. When defining several vehicle signals, choose a different combination of **Signal Source** and **Connector Number**, **Input Number**, or **SSL Position** for each configured vehicle signal.

3. Select the **Input Type** "event".

If necessary, set resistor **Pull-Up / -Down**. This entry is related to the digital inputs IN5 (X02-6, see chapter 2.4.3) or IN7 (X11-2, only PCU-220 and PCU-250, see chapter 2.4.9).

Select an event in the lists **Event On Rising Edge** (input state goes from low to high) and **Event On Falling Edge** (input state goes from high to low).

Typically there are pairs of events, e.g. "Wheelchair on board" and "Wheelchair unload". If you want to register both events select one event for the rising and the other for the falling edge.

If you only want to register one event select this event in the proper list and select "No event" in the other one.

Definition of the input types Extra 1 to Extra 8

Select the generic input types Extra 1 to Extra 8 when signals should be used, which cannot be mapped by the common input types or the input types Odometer Input and Event. Which of these generic input types should be configured, is defined in customer-specific projects.

1. Click on the button **New** to create a new **Vehicle Signal**.
2. Define the input source:
   - Choose the **Signal Source** of the vehicle signal, e.g. "PCU digital input", "network input", or "INP-450".
   - Depending on the chosen **Signal Source**, one of the following parameters must be defined:
     - **Connector Number** (this is the input number IN**x** and not the PIN number Xnn)
     - **Input Number** and **SSL Position** (INP-450 only)

Note: Each input source can only be chosen once. When defining several vehicle signals, choose a different combination of **Signal Source** and **Connector Number**, **Input Number**, or **SSL Position** for each configured vehicle signal.

3. Select one of the **Input Types** "Extra 1" to "Extra 8".

If necessary, set resistor **Pull-Up / -Down**. This entry is related to the digital inputs IN5 (X02-6, see chapter 2.4.3) or IN7 (X11-2, only PCU-220 and PCU-250, see chapter 2.4.9).

4. Set the **Invert** behavior (default: high value means "on" = not inverted).

3.10 Configuration > Positioning Data

With the page **Configuration > Positioning Data** you can configure the sampling of the position via an internal receiver or external GPS-receiver.

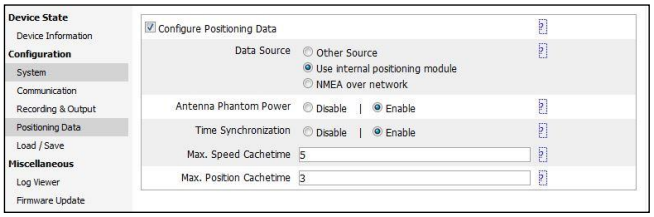


Figure 61: Configuration of the positioning data settings

If the PCU is equipped with an internal GPS receiver (e.g. Navstar, Glonass) or is connected to a GPS receiver via a network (data source **NMEA over network**), the system can obtain the position and time data directly via the satellite-based positioning system. To do this, activate the **Configure Positioning Data** check box.

The PCU can obtain positioning data via an internal module (Navstar or Glonass is available), via an external source (e.g. IBIS or a third-party system via DILAX interface DCP Level 2) or via an external GPS receiver over network. An external GPS receiver sends the positioning data in NMEA (National Marine Electronics Association) format over the local network (Ethernet) and the PCU receives this data.

When the internal GPS receiver should be used for position determination, activate **Use internal positioning module**.

For active GPS antennas enable **Antenna Phantom Power**. This supplies the signal amplifier of the antenna with the required power via the antenna cable. When this option is not activated the GPS reception may be incorrect or insufficient.

The system clock of the PCU can be synchronized with different reference time sources (see chapter 4.1). When **Time Synchronization** is enabled, the PCU receives time data directly from GPS. The coordinates of the current position are recorded in WGS84 format.

Note: Please note that the internal GPS module may need up to 30 minutes at first starts to execute a first position recognition. This behavior is normal and equal to known systems with GPS support (e.g. car navigation systems). At further system starts this procedure is faster and a valid GPS signal will then be available within a few seconds.

If an ***external GPS receiver*** is to be used for position determination, activate the **NMEA over network** check box.

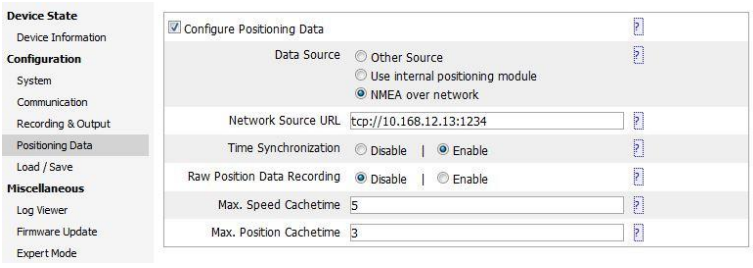


Figure 62: Configuring the settings for position determination for an external GPS receiver.

The external GPS receiver sends the position data and the system time to the PCU via Ethernet in NMEA data format. The necessary network settings must be entered in the **Network Source URL** field. Two transport protocols

are available for transmitting NMEA data over the network: **TCP** (Transport Control Protocol) and **UDP** (User Datagram Protocol).

Protocol	Example	Description
UDP	udp://:1234	The use of UDP is configured with the URL notation **udp://**. The PCU waits for incoming NMEA messages from the external GPS receiver. The IP port at which the PCU has to wait for the messages and to which the external GPS receiver must send messages is also described using the URL notation with a colon followed by a fixed-point number. In the example this is port 1234, described as **:1234**.
TCP	tcp://10.168.12.13:1234	If TCP is being used, the protocol is specified with the URL notation **tcp://**. The PCU connects to the external GPS receiver whose IP address and IP port are specified in the URL notation. In the example, the PCU is connecting to the module at IP address **10.168.12.13** and IP port **1234**.

Table 31: Network configuration for an external GPS receiver.

The system clock of the PCU can be synchronized with various reference time sources (see chapter 4.1). When **Time Synchronization** is enabled, the PCU receives time data directly from the external GPS receiver.

Situations with GPS failure

There may be receiving problems between the PCU and GPS in certain situations, e.g. when the vehicle is in an area where no GPS reception is available (shielded factory hall, driving through tunnels, underpasses and/or bridges).

The most recent valid position data determined by the system is saved in the buffer. In the event of a connection failure, the PCU will obtain the data directly from the buffer memory. The maximum times for buffering the most recent GPS coordinates and the most recent speed value (calculated by the PCU) can be configured in the internal buffer:

Max. Speed Cachetime
Maximum time in seconds for buffering a velocity value
Range of values: [0...900 s], Default: 5 s

Max. Position Cachetime
Maximum time in seconds for buffering GPS coordinates
Range of values: [0...30 s], Default: 3 s

The correct values for the buffer times can have a decisive effect on the quality of the recording data. Distance values are usually calculated using the tachometer or odometer signal. If a tachometer or odometer signal is not available, the PCU calculates the distance values based on the GPS data, accessing the data stored in the buffer if the GPS connection fails. If the time values for intermediate buffering are too low or if no valid data is available, a calculation cannot be made.

With these parameters, the number of recorded way points with invalid positioning data (marked by "n/a" in recording data) can be minimized (see 3.16.1 for details about way points). In the majority of cases the default values are sufficient. Optimal values for buffering times depend on operating conditions of the vehicles (line management, etc.) and can only be determined by empirical tests.

3.10.1 Choosing a Positioning Data Source

When the PCU is equipped with an internal GPS module which supports both, the American NAVSTAR as well as the Russian GLONASS navigation system (see 2.4.7), the type of the navigation system can additionally be selected in the configuration. The internal GPS receiver will then be switched into the working mode of the chosen system.

Note: If GLONASS is chosen data is only taken from GLONASS positioning system, which may affect the time to first fix (TTFF).

3.10.2 Recording of Raw Position Data

Recording of raw position data is optional and available for DLX3 and CSV data recording (see also 3.16). This function can be activated on a master PCU by enabling the **Raw Position Data Recording** option as soon as the data source **Use internal positioning module** or **NMEA via Network** is selected.

When recording of raw position data is activated, the PCU can be used as GPS tracking system. The coordinates from GPS data are recorded internally in a separate file (*.NAV). The format used for recording is described in the "GPS Data Recording" specification (at the moment only available in German). Recorded data is transferred to land side analogue to DLX3 data or csv-data per FTP (see chapter 3.13) Data is stored cyclically by using the configured **Recording Interval**. Generation and transfer of data is analogue to the procedure for DLX3 recording data.

Notes: Raw position data recording is not available in **Client Mode** and in **Master Mode With DCP Level 4**.

Raw position data recording should only be used for project-specific applications or for analyzing purposes. Activating this function leads to higher data transfer and causes higher communication costs. Before using this option check the conditions of your mobile contract (limits for data transfer).

For recording raw position data, data recording must be activated and configured (see chapter 3.16). File closing rules configured in chapter 3.16.1 are also valid.

The maximum data volume per recording file can be calculated in consideration of the recording length and the recording interval.

Example calculation for a recording of one day:

Recording length:	t = 86400 sec (60 seconds x 60 minutes x 24 hours)
Recording interval:	Δt = 2 sec
Block size:	26 Byte

Therefore, a maximum data size of 1,123,200 Byte (approx. 1.07 MB) can be expected at a recording length of 24 h.

3.11 Configuration > Communication > GSM

Use the page **Configuration > Communication > GSM** to configure the communication settings of the internal GSM module.

If the PCU contains an internal GSM/GPRS/UMTS communication module activate the **Configure GSM** check box to use this module for data transfer. The PCU will then send data via the existing GSM/GPRS/UMTS connection to the destination addresses (land side server).

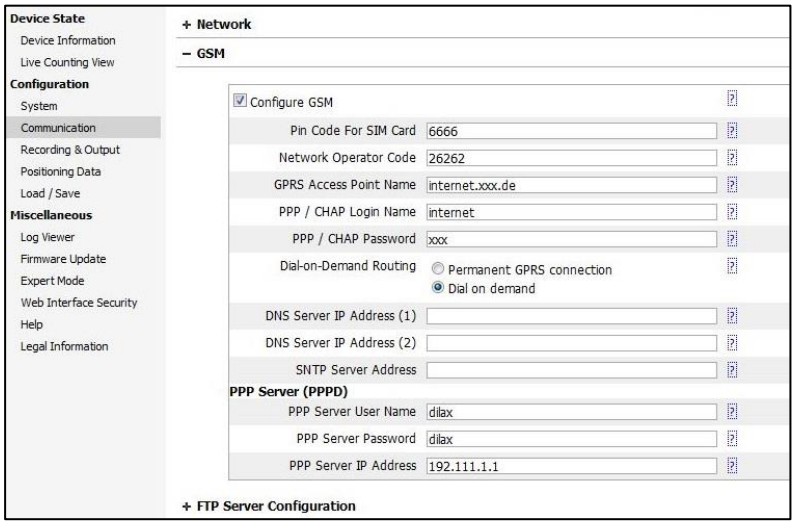


Figure 63: Configuration of the GSM/GPRS communication

3.11.1 Defining Provider Settings

1. Open the **Provider** area to define settings.
2. Enter the PIN code of the used SIM card into the **Pin Code For SIM Card** field. For deactivated PIN code, enter "NONE" into this field.

The **Network Operator Code** field is mandatory and must always be filled out. Enter the code of the network operator (five or six-digit numerical code) which consists of the Mobile Country Code (MCC, three-digit) and the Mobile Network Code (MNC, two or three-digit). The complete code is entered without spaces. Examples:

310240 – T-Mobile USA
23400 – O2 UK Ltd.
26201 – Telekom Deutschland GmbH

For unknown **Network Operator Code**, enter "home" into the field. Then the PCU will then use the network operator code which is stored on the SIM card.

A list of international network operators is available at: http://www.itu.int/pub/T-SP-E.212B-2011

Mobile Data Roaming

From firmware version 1.11.0 on the mobile data roaming function is supported. For automatic selection of the network operator during dial-up to the mobile phone network choose **Yes** at **Allow Roaming**. The PCU will then automatically change to a GSM roaming provider when the standard provider is not available during dial-up to the mobile phone network.

You can use this function when the vehicles operate in international traffic (international roaming) or when a subnet of a local network provider should be used (national roaming).

Notes: Roaming connections cause additional communication costs. Exactly check the conditions of the mobile communications contract before you choose a network provider/mobile communications contract. Ask the appropriate provider beforehand about additional costs resulting from mobile data roaming usage.

Activation and usage of the mobile data roaming function are the sole responsibility of the end user. DILAX does not warrant or shall not be liable for additional costs or fees.

According to the EU roaming regulation III ((EG) No. 531/2012, valid since 2012-07-01) the network operators and providers are obliged to limit the costs resulting from roaming connections. Therefore network operators use a "cut-off" mechanism which disconnects the connection and blocks further connections when a specific cost limit (50 EUR) is reached.

Download of the EU roaming regulation III at:
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:172:0010:01:EN:HTML

According to contractually details of the mobile communications contract there may be situations within an accounting period in which data connections are blocked by the network operator. In such cases, the PCU is no longer able to dial-up to the mobile phone network and cannot establish connections for data transfer. For this reason no data (DLX, live/station tracking data) can be sent.

These situations are not a malfunction of the PCU or the automatic counting system because the establishment of a connection is blocked by the operator of the mobile communication network. Directly contact your network operator or mobile communication partner and apply for a cancellation of the lock or a change of the contract.

3.11.2 Defining Data Connection Settings

1. Open the **Data Connection Settings** area to define settings.
2. Enter the **PPP / CHAP Login Name** and the **PPP / CHAP Password**.

Note: Some providers do not require a login name and a password. In this case leave the login name empty and the password's check box unchecked.

3. Use the **Dial-on-Demand Routing** option to configure the behavior of the connection establishment. When you activate the **Permanent GPRS connection** option, the PCU establishes a permanent connection via mobile phone network. On the other hand, when you activate the **Dial on demand** option, the GPRS connection will be established for each data transfer and disconnected after data transfer. The connection is only established when data should be transferred by the PCU (transfer of the DLX3 file with counting data at a specific time or at the transfer of real time data). When live/station tracking applications are used it could be better to choose a permanent connection. The correct configuration of the **Dial-on-Demand Routing** parameter depends on specific application scenarios and should be checked accurately.

Notes: In most cases it is sufficient to activate the **Dial on demand** option.

A **Permanent GPRS connection** is only necessary when the PCU should send data in real time to land side (live/station tracking, GPS tracking, etc.). Please note for configuration:

While a permanent connection is established, a direct remote access to the PCU is not possible because the GSM interface is permanently occupied by the GPRS connection and the PCU cannot receive incoming calls. That's why as of firmware version 1.10.0, the PCU searches for

configuration scripts in the configured FTP directory once per hour. These configuration scripts can be used to change the configuration. Hereby a permanent connection can be stopped for performing service activities via remote access, if necessary. Afterwards the function must be activated again by a changed configuration.

A permanent Internet connection increases data transfer and communication costs. Check the conditions of your mobile communication contract (data transfer limits) before using this option.

Chapter 5.7 explains how errors can be recognized. In case of data transfer problems check the details of the existing mobile communication contract (data transfer active, roaming cut-off, correct APN or MLC/MNC setting).

3.11.3 Defining Network Settings

1. Open the **Data Connection Settings** area and within the **Network Settings** area to define settings.

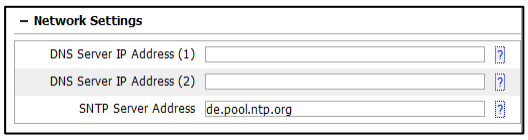


Figure 64: Defining GSM/GPRS network settings

If the host name (domain name) should be used instead of the IP address, an external DNS server is necessary for name resolution and conversion into an IP address. In most cases, the provider is sending the address of the DNS server to the PCU during GSP connection establishment so that name resolution can be done automatically. But sometimes this is not the case. That's why we recommend to configure at least one DNS server when host names should be used instead of IP addresses. For configuration use the **DNS Server IP Address (x)** fields.

When the PCU's system time should be synchronized by a time server via GPRS, the IP address of the time server (NTP or SNTP) must be entered into the **SNTP Server Address** field. See chapter 4.1 for detailed information about synchronizing the time. Lists of available NTP/SNTP server names are available in the Internet. In the rare event that the GPRS provider is providing the SNTP name during connection establishment, enter the value "auto" into the **SNTP Server Address** field.

Note: The SNTP server should be available permanently to ensure reliable setting of system time. Select option **permanent GPRS connection** to ensure that the SNTP server is permanently available.

3.11.4 Defining GSM Security Settings

P1. 1.10.5.1.4

1. Open the **Data Connection Settings** area and within the **GSM Security** area to define settings.

By default, incoming GSM/GPRS connections are rejected by the device. If necessary, access can be granted with the settings in the **GSM Security** area. The TCP/IP protocol is used.

Warning: Incoming connections to the PCU are a potentially high security risk. Only allow accessing the device from the outside, if this is really necessary.

Note: The settings only affect incoming communications. They do not affect connections which are started by the PCU itself or any dial-in connections (see 3.11.5).

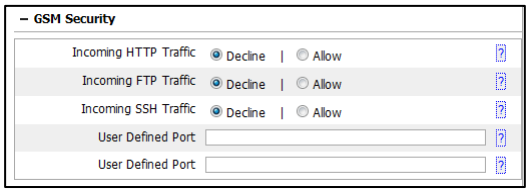


Figure 65: Defining GSM/GPRS security settings

2. Set the **Incoming HTTP Traffic** option to "Allow" to grant accessing the web interface of the PCU via a GSM/GPRS connection.

Warning: It is recommended to secure the access to the web interface by a password (see chapter 3.3) in order to only allow authorized persons to change parameters.

3. Set the **Incoming FTP Traffic** option to "Allow" to grant accessing the FTP server of the PCU via a GSM/GPRS connection.
4. Set the **Incoming SSH Traffic** option to "Allow" to grant accessing the SSH server of the PCU via a GSM/GPRS connection.

If necessary, two user defined ports (UDP) can be configured. On these ports all incoming UDP/TCP connections via GSM/GPRS are allowed. Valid values are 1-65535.

3.11.5 Defining Dial-In Settings

1. Open the **Dial-in Settings** area to define settings.

Note: PCUs which are equipped with a 3G modem do not support dial-in.

For functional tests or service tasks, a remote access to the PCU from "outside" can be realized via a remote connection. Therefore, the integrated PPP server of the PCU must be activated in the **Dial-in Settings** section and access data for dial-up must be configured. Leave all fields empty to deactivate this functionality.

Note: PPP connections are superordinate to GSM/GPRS connections. PPP connections are still possible even if the **Incoming HTTP Traffic** is set to "Decline" in the **GSM Securiy** area.

2. Define a **PPP Server User Name** and a **PPP Server Password**. Both are necessary for the remote access to the PCU.

The **PPP Server IP Address** is the IP address of the PCU which is used for dial-up to the device from the outside.

3. When the connection to the PCU is established the web interface of the PCU can be accessed by entering and confirming the **PPP Server IP Address** in the address line of the web browser (e.g. http://192.168.0.1/?long_timeouts=1). It is suggested to use the following default values:

PPP Server User Name:	dilax
PPP Server Password:	dilax
PPP Server IP Address:	192.168.0.1

The IP address of the client PC is generated automatically on the basis of the configured IP address of the PCU (last block of PCU IP address + 1). Example:

PPP-IP of the PCU:	192.168.0.**1**
IP of the client PC:	192.168.0.**2**

Warning: Note down the **PPP Server User Name** and the **PPP Server Password**. A remote connection to the PCU cannot be established without these values. You would have to configure the device again via a different connection (e.g. a direct access via the vehicle's network).

In case of loss of dial-up data, remote access cannot be unlocked by the manufacturer too.

Note: Using the authentication data of the integrated PPP server only protects the incoming network connection to the PCU. Other access data is used for the web configuration which have to be configured separately (see chapter 3.3).

The extension ?long_timeouts=1 allows a remote access via a very slow GSM connection. Connection errors would occur without using this extension.

Use the default value for the **PPP Server IP Address**. Only change this value in case of address conflicts (e.g. when the same private address space 192.168.0.x is used in local network).

The subnet mask is automatically configured to the value 255.255.255.0 and cannot be entered manually.

3.12 Configuration > Communication > FTP Server Configuration

The PCU has a build-in FTP server which allows a remote access to data stored in public directories by using an FTP client program (e.g. for copying data into a local directory).

To realize a remote access to the directories of the PCU via FTP open the **Configuration > Communication > FTP Server Configuration** page, activate the **FTP Server Configuration** check box and enter **Username** and **Password**.

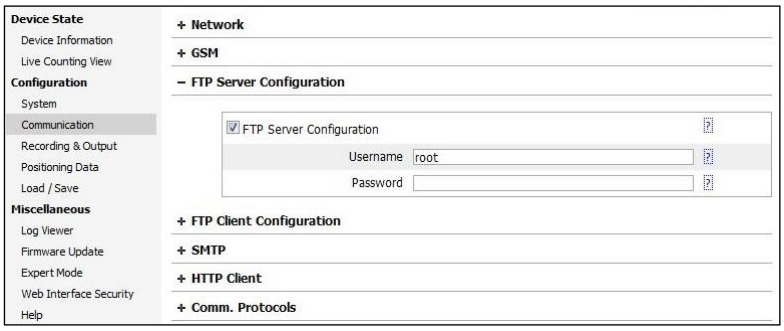


Figure 66: Configuration of the build-in FTP server

The following directories can be accessed via the build-in FTP server:

Directory	Content description
data	Counting data record files.
log	Log files displayed in the log viewer.
master	Reserved for later use.
system	Reserved for later use.

Table 32: Via FTP accessible directories of the PCU

Note: When remote access should be used, choose the transfer mode **Passive** at the **Mode** parameter in the **FTP Client Configuration** (see chapter 3.13).

Note: When you are using remote access, you are responsible for deleting already fetched files from the "data" directory in order to keep the number of files in this directory manageable. When you don't delete files, new files will be added continuously. If the number of files exceeds the limit of 99, the PCU will automatically delete the oldest files.

3.13 Configuration > Communication > FTP Client Configuration

When the PCU should automatically copy counting data via an FTP connection to another server (within the vehicle or at land side) configure the FTP client. Open the **Configuration > Communication > FTP Client Configuration** page and activate the **FTP Client Configuration** check box.

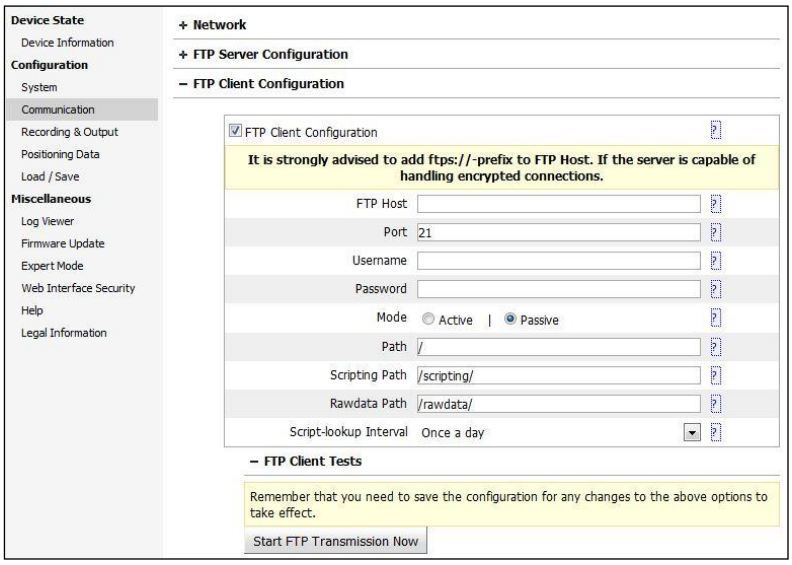


Figure 67: Configuration of the build-in FTP client

Enter the access data (**Username** and **Password**) for the remote FTP server.

Attention: Special characters can affect the PCU's functionality.

Never use special characters in passwords or user names. If necessary, ask your IT department to change access data appropriately. Special characters can, for example, avoid a correct execution of automated update scripts via remote access.

Avoid special characters (e.g. Ü, ä, *, $, § etc.). Only use letters (a,b,c ... A, B, C etc.) and digits (1, 2 ,3 etc.). Use underlines instead of spaces.

Select an FTP Host with or without encryption:

The PCU supports data transfer encoding by the configured FTP server.

Unencrypted connections: Enter an IPv4 address (e.g. 192.168.2.1) or a DNS name (e.g. my.server.com) into the **FTP Host** input field.

Encrypted connections: Use the ftps:// prefix when entering an IPv4 address (e.g. ftps://192.168.2.1) or a DNS name (e.g. ftps://my.server.com) into the **FTP-Host** input field. When a connection is established, the PCU will check if the remote station supports SSL encryption. If not, the connection will be rejected.

Select the FTP mode:

Active: The PCU informs the FTP server on which port it is listening for incoming data connections. The FTP server initiates the data channel for file transport.

Passive: This is the preferred mode. The PCU receives necessary connection data from the FTP server and then initiates the data channel for file transport.

Note: In situations where the client is behind a firewall and unable to accept incoming TCP connections, **Passive** mode may be used.

Enter the basis directory into the Path input field.

On the remote FTP server, the following directories must exist or be created:

Directory	Content description
rawdata	Storage place for counting data record files
scripting	Storage place for test files, scripts and update packages (PCU firmware)

Table 33: Directories at the remote FTP server

Note: Ensure that the necessary write and read permissions are configured for the directories on the FTP server. Otherwise the PCU could not access the directories and data exchange would not be possible.

Changing the scripting and rawdata directory

When the directory structure is already defined or cannot be changed, the designations of the "scripting" and "rawdata" directory can be specified in the fields **Scripting Path** and **Rawdata Path**. In all other cases leave the default values of these fields untouched. The directory names must be specified as a path starting with the root directory specified in the **Path** field.

Example 1: Rawadata and scripting directory with different directory structure.

Directory	Path at the FTP server	Field	Value
root	/vehicles/2033/	**Path**	/vehicles/2033/
rawdata	/vehicles/2033/data/countings/	**Rawdata Path**	/data/countings/
scripting	/vehicles/2033/firmware/	**Scripting Path**	/firmware/

Table 34: Directories at the remote FTP server – Example: Rawdata and scripting directories with different directory structure

Example 2: Storage of all data in the same root path.

Directory	Path at the FTP server	Field	Value
root	/	**Path**	/
rawdata	/	**Rawdata Path**	/
scripting	/	**Scripting Path**	/

Table 35: Directories at the remote FTP server – Example: Storage of all data in the same root path

To test the build-in FTP client configuration click on the **Start FTP Transmission Now** button. Further details see chapter 5.10.

To check the presence of a script on the configured FTP server, a **Check interval** can be set. The default value is "once per day".

3.14 Configuration > Communication > SMTP

The PCU offers the option to automatically generate error reports and send them via e-mail to several e-mail addresses. The report will be sent automatically once per day.

The error report contains error messages and warnings occurred during runtime of the system (e.g. critical reboots executed by automatic system monitoring). The PCU's firmware is continuously updated. That's why the error messages may vary depending on the firmware version used.

1. Open the page **Configuration > Communication > SMTP** to configure the SMTP e-mail settings.

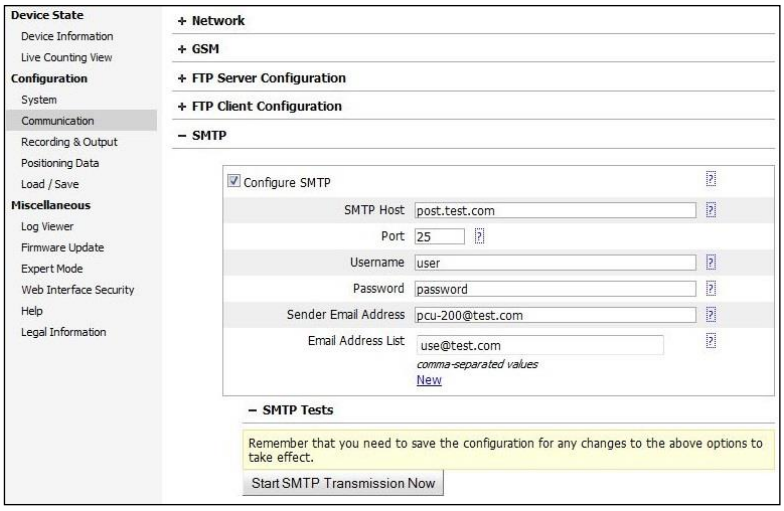


Figure 68: Configuration of the SMTP client

2. If the e-mail server requires an authentication, the values **Username** and **Password** must be defined. If no authentication is necessary, these fields can be left empty. Ask the responsible system administrator for the necessary values.
3. Enter one or several receivers into the **Email Address List** field. Several addresses are separated by a comma. Alternatively, use the **New** button to enter further addresses.
4. To test the SMTP configuration save the configuration settings on the device and then click on the **Start SMTP Transmission Now** button. Further details see chapter 5.11.

3.15 Configuration > Communication > HTTP Client

In normal operating mode of the PCU, data is captured and recorded (DLX3) during operation time and sent to an FTP server (configuration as master) once per day. In client mode, no recording is done in normal operating mode. Data is requested and recorded at each counting operation by a third-party system via network or serial connection.

In addition it is possible to send counting data and further information to a server in real time. This live/station tracking function can be used to provide data to a further system in the vehicle or at land side during a trip for further processing (e.g. vehicle location, for information or fleet management systems).

Note: Live/station tracking data can only be generated and sent when the PCU is configured accordingly and when a valid time is available. A time synchronization must have been executed successfully. Depending on the configuration, it is possible that the generation of live/station tracking data is only then generated when the vehicle is moving and a station is reached.

Example: A vehicle synchronizes its time per GPS. During start-up it is located in a hall where no GPS is available. Therefore, time synchronization is not possible and the PCU cannot generate live/station tracking data. Generation will not start until the vehicle has left the hall, a valid time has been supported by the GPS system, and the PCU has executed time synchronization successfully.

Note: Please note that the usage of this function causes a higher data transfer and therefore higher costs (transfer via GSM/GPRS). Before using the function, check the conditions of the existing mobile communication contracts and contact your mobile communication provider, if necessary. DILAX does not warrant or shall not be liable for additional costs or fees.

The transfer of real time data to the server is done via DILAX Counting Protocol Level 3 (DHCP L3) by using the Hypertext Transfer Protocol either unsecured (HTTP) or secured (HTTPS). To use this function configure the server which receives the data and the transfer parameters on the **Configuration > Communication > HTTP Client** page.

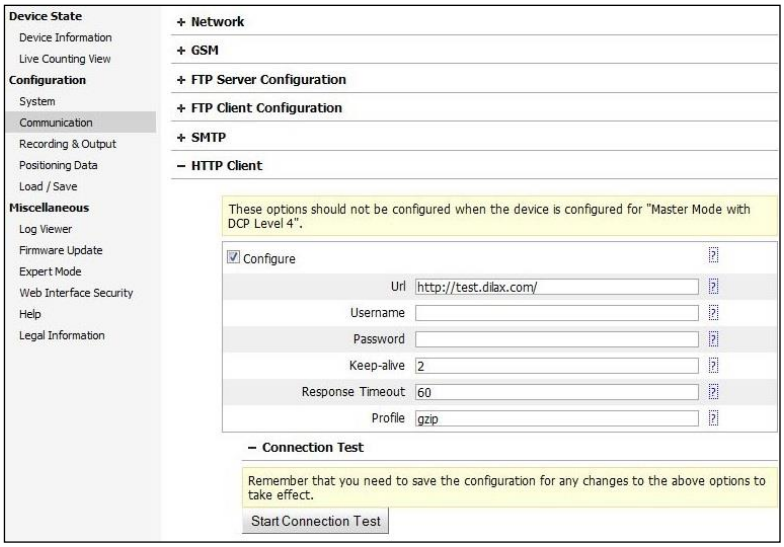


Figure 69: Configuration of the HTTP client

Enter the address of the HTTP destination server into the **Url** field. The value must contain the protocol identifier http:// . When the standard port 80 should be used for data transfer, the port must not be entered together with the address. If you are using a different port, you have to enter the port separated by a colon. For the address, the IP address or the hostname of the server can be used.

Examples:

http://192.168.10.95/	or	http://test.dilax.com/	(using standard port 80)
http://192.168.10.95:8080/	or	http://test.dilax.com:8080/	(using port 8080)

If the HTTP destination server receives data via a specific resource, this must be additionally entered in the URL. Example:

http://test.dilax.com/test_push.aspx

Note: It is recommended to use the IP address (IPv4) as URL. The PCU only supports IPv4 addresses, IPv6 addresses cannot be processed.

If the host name is used, an external DNS server is necessary for the address resolution (host name to IP address) which must be known to the PCU and configured in the PCU (see chapter 3.6).

When the input fields **Username** and **Password** are configured, the PCU working as the HTTP client will execute an authentication with these values during connection establishment. Otherwise the connection is established without authentication.

By entering a time value into the **Keep-alive** field you can define the maximum time the PCU holds a connection to the HTTP server for data transfer in order to send further requests. The value is optional and must be entered in seconds.

Notes: Please use a similar but marginally smaller time value than the time value used for the HTTP server at the receiver side. Incorrect settings can cause instable connections and connection failures between the PCU and the server.

Before configuration, ask the IT department of the company operating the HTTP server for the necessary information of the **Keep-alive** value to be configured.

If it is not possible to identify the exact value of the server, use the standard value 0 (zero). With this value, the PCU holds the connection to the server active for 60 seconds.

For instable connections like GPRS use a small value of 2... 10 seconds.

Some HTTP servers process the **Keep-alive** time incorrect. In such cases, every second connection fails. This can be prevented by setting the **Keep-alive** time to 2 seconds.

With the **Response Time** you define the maximum time value which the PCU is waiting for an answer from the HTTP server. The default value of 60 seconds should be used for this parameter. Sometimes the answers from the server are delayed. In such situations increase the value to avoid problems.

Additional commands can be entered into the **Profile** field. With these parameters it is possible to adapt the standard behavior of the HTTP client of the PCU. Several commands can be entered separated by a comma. The sequence can be chosen freely. The following commands are supported:

Command	Default behavior	Changed behavior
gzip	Data will not be compressed for transfer.	Data will be compressed for transmission (recommended for GPRS transmissions). The HTTP server must be able to decompress the data. When you are unsure if the receiving server can handle compressed data, do not use the gzip command. There is the risk that data cannot be processed by the server.
dcp_ping	dcp_ping is not active.	When the **Keep-alive** time is reached, the HTTP client sends a DCP ping request to the HTTP server. This restarts the keep-alive timer of the HTTP server and the connection persists (for more information, read the DCP specification Level 3).

Table 36: Profile commands in HTTP client configuration

When all parameters are set and saved, you can check the setup. Click on the **Start Connection Test** button to send test data to the HTTP server (for details see chapter 5.12).

3.15.1 Secure data connection via HTTPS (data encryption)

The PCU offers the possibility to encrypt the communication channel for data transfer. This function can be used to prevent so-called man-in-the-middle attacks by unauthorized persons. In this case, the server (in the vehicle or at land side) and the client (PCU) are communicating via a secure HTTPS connection and are using certificates during connection establishment for authenticity check.

The function can only then be used when the data transfer is activated. Therefore, the PCU must be configured as HTTP client (see chapter 3.15). If the URL is given with the https:// protocol, the build-in HTTP client of the PCU automatically uses the HTTPS protocol for communication. In this case, the communication is encrypted independent from activated/deactivated certificates in the **Certificates** area of the web interface.

Warning: The usage of data encryption methods may be limited by national laws (especially USA, Russia). Before using this security function, find out more about the legal framework.

The usage of this function is in the responsibility of the end user. DILAX gives no warranty.

For using the secure transfer, ensure the HTTPS communication is activated at the destination server. In case of doubt ask the IT department of the company operating the server.

Activation/Deactivation

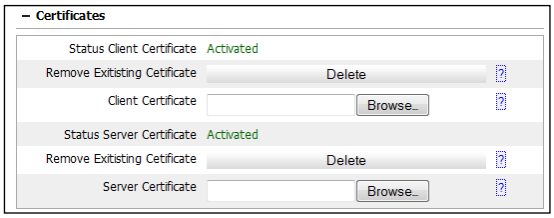


Figure 70: Definition of certificates during configuration of the HTTP client

To activate the usage of certificates, upload the certificate file to the PCU in the **Certificate** area of the web interface. At upload an already stored certificate file will be overwritten by the new certificate file. For deactivating a certificate click on the appropriate **Delete** button and the appropriate certificate file will be deleted from the PCU.

Notes: Deleting certificates deactivates the function. This step cannot be undone in the configuration. In order to activate the function again, a new certificate file has to be uploaded. The PCU must be rebooted before the uploaded certificate is definitely activated.

The PCU does not check the certificates for correct structure and correct content. You have to ensure a correct structure and content by yourself. For this check you can use free OpenSSL tools (see also http://www.openssl.org/).

The PCU does not provide a maintenance function for certificates. Ensure that the certificates are always up-to-date and valid. The certificates must not be listed in official black lists.

For standard browsers the operating system provides a list of CA certificates and ensures periodic security updates. The PCU does not update certificates. Maintenance has to be done by the end user of the automatic passenger counting system. When certificates are invalid or become invalid, the certificates in all PCUs of the whole vehicle fleet have to be updated.

By using certificates, the connection behavior between the client (PCU) and the server (in the vehicle or at land side) is controlled. The status (active/inactive) is displayed at the web interface of the PCU and has the following meaning:

Certificate/Status	Activated	Deactivated
Server Certificate	The verification of the server's certificate is activated. If the HTTP client rejects the certificate of the server, a connection will not be established. Otherwise, the following data transfer is encrypted.	The verification of the server's certificate is deactivated. The HTTP client trusts each web server. The connection to the server will be established but any data transferred will be encrypted.
Client Certificate	The HTTPS client authentication is activated.	The HTTPS client authentication is deactivated.

Table 37: Status of certificate file

Verification of the server's certificate

The HTTP client checks during connection establishment to the server if the server can be trusted (standard behavior). Therefore, the **Server Certificate** must be uploaded to the PCU first. This file contains the public certificate signed by the Certification Authority (CA) which is used by the operator of the webserver for signing the server certificate.

When a connection is established, the HTTP client trusts in principle each web server sending a certificate signed by the same certification authority.

During connection establishment the PCU receives the certificate of the web server and matches it with the certificate uploaded to the PCU. Thereby it is checked if the certificate is valid and if it was signed by the certification authority. When this check was successful, the client trusts the web server and the data transfer is done encrypted. Otherwise no data transfer takes place.

Attention: The PCU uses the current system time for validation check. When the system time of the PCU is not up-to-date, the check may fail even if the certificate is valid. Therefore ensure that the system time of the PCU is up-to-date for the validation check (connection establishment). See chapter 4.1 for detailed information about synchronizing the time.

Structure of a Server Certificate File

The CA certificate must be structured according to the X.509 standard (see also http://tools.ietf.org/html/rfc5280) and the file must be encoded in *.PEM format (see also http://en.wikipedia.org/wiki/X.509).

The *.PEM format allows storing several CA certificates in one file. The HTTP client (PCU) supports searching the CA certificate list. The following figure shows an example of a Server Certificate File with one CA certificate.

Figure 71: Example of a Server Certificate File in PEM format containing the X.509 certificate of a CA

HTTPS Client Authentication

The HTTPS client authentication is an extension of the HTTPS protocol. During connection establishment the server checks if the client can be trusted. For using this function it is required that the authentication function on the server is activated and that a valid **Client Certificate** is uploaded to the PCU (as client). When the HTTPS client authentication is activated at the server, the server asks the PCU for a client certificate during connection establishment. The PCU sends the uploaded certificate to the server.

The server checks if the certificate is up-to-date and reliable by using a certificate list with certification authorities (CA). When the client certificate was signed by one of the listed certification authorities, the check was successful and the server trusts the client. The connection will be established and the data transfer can be executed in encrypted form.

If the PCU cannot send a client certificate (e.g. it was not uploaded) or if the client certificate was not signed correctly, the server rejects a connection and data cannot be exchanged.

Structure of a Client Certificate File

Because the operator of the web server demands the usage of HTTPS Client Authentication, he is responsible to prepare the Client Certificate File. The Client Certificate file must contain:

The private RSA key (see also http://en.wikipedia.org/wiki/RSA_%28algorithm%29) for the HTTP client to encrypt the Client Certificate.

The X.509 Client Certificate (see also http://tools.ietf.org/html/rfc5280), which is signed by the CA the web server trusts.

Both parts of the file are encoded in the *.PEM format (see also http://en.wikipedia.org/wiki/X.509).

Figure 72: Example of a Client Certificate File in PEM format containing the private RSA key and the X.509 certificate of the client

When the private RSA key was created with a **Password**, the HTTPS client needs this password to decrypt the key itself. The password has to be manually added to the client certificate file by using a text editor. Therefore, a line with the following format must be added to the beginning of the file:

Password:<Password>

<Password> must be replaced by the actual password. Ensure that there are no additional blank characters behind the password.

Example:

```
Password:x1qf58H
-----BEGIN RSA PRIVATE KEY-----
UWWS2au3Y7KnASV3Lcjym21qPvfwSafwZAgn5Es0I9uxCPtAyk5eA/9a/7+U1IGT
h7Ct4yYPjAuClyaCVD/TIESd1SFgntCjj7h6bt/oS1ZtewjU12d0UFRaeeWh6NGK
CcX4T+FyJ6WOntDaGMYpzbbtNdmRrN1jx9Pljz/hyMXWBJ6XNWYGEAIQP6gbNYFj
tg0/88lkCSCczmjO9utCwxKmbN8HQ53502p7IIZpM3uMX/zZZNyHc0/uRwauXaRz
IjCTXRir+bV3n63iYGP5VOGnTHCgY5YDGowlO4dveNff18bD7Tj411xs0Y7puxD2
I8Z+6FhqIoVv1moZAoH29UHtQRbhZj0FWqOkmFsW1MmWGKASH9NwRGGmw1XZ8pVG
fWA/Xdo91ajNnEoueFbUBwFN3VSQgFmuAUmhZDc3qcscNbxNgAW7BR3oipMqUKJz
lIBRkA/M23rmZYaD+FbDLuWQPJvcYjvIntT8EoYTKQ7CEgm930aUnzTVhf6DSkIJ
99RCMrr6nUGg4N4lio+xNulgHF1MucQeBiVa66FZoUnBdyYyMr2yO+TZg+Tm5QS6
pT3vaf0rB7cPeINLL2vqpIRxX4BWqIs7cTYuqitD4Th3TVZUjlhngCv1i8WrNdiG
BPgfHLmsmNd0HR7GFdNiFfBSPclkgLDXW4pxoukv4VacymCL1sg3qBUYjPB+9QCu
NjooI5DxK+kGSC46RZ9/UHD4X1SS/6i/AXPk9rAcD7RdcU42OUYKYwlyAEJjGt7i
mip5ATqmmRNVKNsbVxmvx1DNPJwcGpVdnWdA482bgDARXs95OetbFtisHL8Njf/X
tz5I6e/3KVFg5mcc1ThLneBrTn8hyfXs8muD0vl5QEUjPgou3Y7xoJOdniXU0Bw9
IiziIQuuPEreM4tFHdU1nh2vrZNoMWal22bhRJ5tj8kQTqMJsQBV41glbbG43GMo
1khnQG0EBgb2RDRK27GR89qDrkXFcL5Eh6El7AwYt2OkSvrkCYnwd44LadAQwyk4
XLduKNr00uPS1aPc3VD7Pak/exBM5EozFjg6iYQjJC+0DgeVfJOI1Fh486UUT4kX
ub1kii9CEld9I0/PJE/u89Qr7EcWq+fTW9l2Mn3yl71bG/4E6syvRebLjGKQMXR+
0PW1s+zP5lOLu6OfiGEY2GuUyrvQhVAUcHnOQxmkOG6Y6NPWczPPx112yjPmw5Ju
xgM4IEJL0//Jo3bpvLU5JfG/Lp4q0zig+nIupU75OmVNsl1NRcZPeziIeh3OeLMp
za0j+MuOmzzV0p+QySMeJ9JU0Gu14D7KasaShtaW0dOibvHTd5bF05fQOpF2oAbQ
b+ER+TV3BNcApITJ7gOS9ls3yrmDSiFbPbmsk8JN7Y6EtQjuiNvdGpa8I99ksSom
HZIhmx2SKJtw1BaWcQ4YqivjteYISE68QzRHsm6wQWRcakQjg9U+Thv/D0elIR30
2BC9lCfg3DkoR//LjBNK0Zxr5YuggVJ0G0wbc+vR9twAJqBNoJt+zR/5ikCO7guz
+9a6E1rgO5adBQYujJEXlH9mCFHHpMBp7C1C5KX3Gc095YT/OsDiljAvBjYSpQLn
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
SUIEJTCCAw2gAwIBAgIIM1HhyWYC6MowDQYJKoZIhvcNAQEFBQAwdTELMAkGA1UE
BhMCREUxFjAUBgNVBAoTDUR1dXRzY2hlIEJhaG4xDDAKBgNVBAsTA1BLSTEXMBUG
A1UEChMOREIgU3lzdGVsIEdtYkgxJzAlBgSVBAMTHkRCIFRydXN0IEN1bnRlciAo
V2ViMi1DQSAyMDA5KTAeFw0xMzA4MjkwNjQxNDhaFw0xNzA4MjkwNjQxNDhaMIGA
MS4wLAYDVQQDDCV0c3Qtc2JybS1yZWdpb3N3LTIwMTMwODI3Lm5vbmNkLmRiLmRl
bFtGnC1ApKyudlAPkfpvTR2C8uhv55QEYk3DZvYcfJsYg+iBPkEcN8Gylz/lKrT/
MRAwDgYDVQQLDAdEaWVuc3RlMRcwFQYDVQQKDA5EQiBTeXN0ZWwgR21iSDEWMBQG
AQUAA4IBDwAwggEKAoIBAQCw99dMNyD2MlAKNKA+H2vcksTBD2KUk1UcOOytX0wG
A1UECgwNRGV1dHNjaGUgQmFobjELMAkGA1UEBhMCREUwggEiMA0GCSqGSIb3DQEB
Rzw1tdiVQTyF++rQa9aIR6QNtWmrK20MJD7S+ctrn0/bJzfahoBRBATP9KvrWTXu
v5TDKZZFnAKWizsrITLyA/a5jNeNB2qvdaT2CEyRrVAVMKdeZixtV1hTZaxQF8dV
lnHrY604PiRl5Q3NHUN7Gm+t/qPVye/0ViJperPRkTMh13KewngNJeATiEC0cmBy
kVPL1OTpNxiSxFHgmzQbgXm0J+ecdncvCmEdQ0oeSBRNkBigLCwenTpuqmugodH7
XtONl+F5a32Suj3bhoODEOGOnaDedoIisjp89lYxsmcrAgMBAAGjgawwgakwHQYD
VR0OBBYEEEaRNeUNVNjMQHMypkNPl2kFjWqOMAwGA1UdEwEB/wQCMAAwHwYDVR0j
BBgwFoAUg7Q+E/Yh9xTYX1twMzhMpR8HyFgwDgYDVR0PAQH/BAQDAgWgMB0GA1Ud
JQQWMBQGCCsGAQUFBwMBBggrBgEFBQcDAjAqBgNVHREEIzAhgR9IZW1rby5Tb2Vo
bmdlbkBEZXV0c2NoZUJhaG4uY29tMA0GCSqGSIb3DQEBBQUAA4IBAQBP8ecBhzQs
Gcqq24lLlnM+gynPCfyyAaUcBuunKgLcXRqgRjiQOPt1QoB8Z7gmgPT0/qCEwELB
bdM82tURHx9gnL88828hRb43KdtVf59hiib/laPx3jeNSjOQuvDHRlWEU8TWXavu
WSyN1Rc2uRI3QrLHj79vKZvnEtcGMWMAnaH/ey8juU9jlWb2irbnlnePvQfzbeMP
wyDonaebsEwKmLqcA84KRx6XPMtRksih9Nqqj5VLuMoJmho5BtfJWBo02/IFw6Fp
A6invZPGaAme
-----END CERTIFICATE-----
```

Figure 73: Example of a client certificate file in PEM format with password, private RSA key and X.509 client certificate

3.16 Configuration > Recording & Output > Data Recording

Use the settings on the **Configuration > Recording & Output > Data Recording** page to start, stop, and configure data recording.

Please note that the settings differ for the usage in mobile and stationary applications.

3.16.1 PCU usage in mobile systems (vehicles)

For the usage in mobile systems, ensure the operation mode is set to **Master Mode with DLX3/CSV** (**Operation Mode** parameter at **Configuration > System > General**, see chapter 3.5). In this mode, the DLX3 format or alternatively the CSV format is used for data recording.

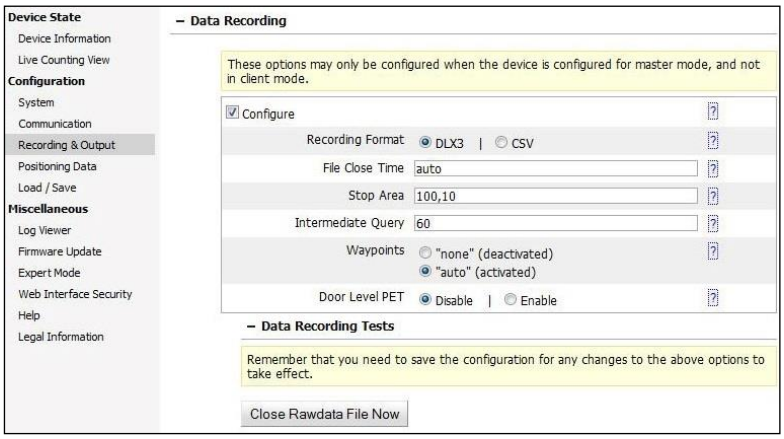


Figure 74: Configuration of DLX3 data recording for a mobile system

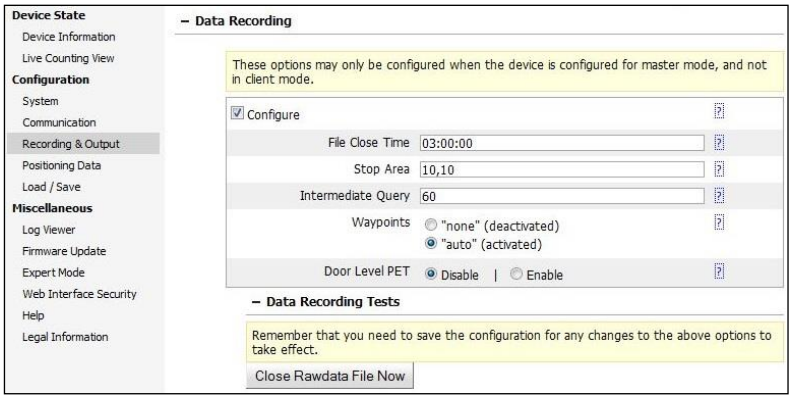


Figure 75: Configuration of CSV data recording for a mobile system

1. Activate the **Configure** check box to record counting data.
2. Select the **Recording Format**: **DLX3** or **CSV**.

Attention: Do not switch the recording format while data is recorded.

Before switching recording data, back up measured counting data which is still on the PCU.

When the recording format is switched and the configuration is saved, measured counting data in old format will be deleted from the PCU. This ensures that there will be enough storage space available for recording in new format.

From firmware version 1.16.0 onwards counting data of stops can also be recorded in CSV format (**C**omma **S**eparated **V**alue). The CSV format is human readable and allows further processing or visualization of the data in spreadsheet programs like MS Excel®.

Note: Counting data is only recorded in CSV format when the counting system is configured with a valid time after 01.01.2000.

If desired, change the default settings of the other settings:

Parameter	Default value	Comment
File Close Time	auto	Local time (not UTC) Recommendation: Fix value 03:10:00 am. **Note:** In any case, avoid a time which lies within the leap hour between winter and summer time and vice versa.
Stop Area	100,10 (meters, seconds)	Size of a station
Intermediate Query	60 (seconds)	Time after arriving a stop at which an intermediate state of incoming and outgoing passengers at this stop is recorded.
Waypoints	none	**Only DLX3** Recommendation: auto
Door Level PET	Disable	**Only DLX3**
Recording Profile	SEP:CP,DOORS:10,PET:1,QI:I,QCI:D,QC:A	**Only CSV** SEP:CP = Separation with a comma (C) as column separator and a point (P) as decimal point. DOORS:10 = Columns for 10 doors will be created. PET:1 = The passenger exchange time for the vehicle is determined during stops at the stations. QI:I = The passenger information data recorded at intermediate query is the current passenger information data. QCI:D = The passenger information data recorded at final query at station with preceding intermediate query is the current passenger information data. QC:A = The current passenger information data recorded at final query at station without preceding intermediate query is the passenger information data recorded at arriving the station.

Table 38: Default values for data recording in mobile systems

File Close Time

The PCU records data of the vehicle's operating day in a DLX3 file. This file has to be closed before it can be sent from the vehicle to the back office. The **File Close Time** parameter defines the point in time (local time) when the file should be closed. You can decide to define a fixed time or to use the "auto" mode. The file will automatically be sent the next time a connection is established to the land side.

When configuring a fixed time (e.g. 03:10:00), avoid a time which lies within the leap hour between winter and summer time and vice versa. Ensure the file is not closed when the vehicle is in motion. This may lead to loosing counting data of a stop.

Note: When the vehicle is not in operation when the file closing time is reached, it cannot be closed because the PCU is not in operation, too. In this case, the file will be closed immediately after the vehicle is in operation again and the PCU has been synchronized with a valid time.

In "auto" mode, the file is automatically closed and thus is ready to be sent, if it is at least 24 hours (DLX3) or 4 hours (CSV) old and if the PCU recognizes the "vehicle not in operation" state.

The "vehicle not in operation" state can be signalized in different ways:

- via an appropriate signal at the digital inputs
- via a network input with appropriate configuration of the vehicle signal "vehicle in operation " (see chapter 3.9)
- via automatic state interpretation by the PCU

Example: The vehicle is not in operation when the PCU does not register any signals pointing to usual vehicle operation for 20 minutes.

Stop Area

The size of the stop is defined. The PCU uses the size to recognize when the vehicle has left a station. Then counting data of this station is recorded.

The parameter consists of two values: "a,b" (comma-separated and without any blank):

a: Length the vehicle has to move to leave the station.

b: Time in seconds the vehicle has to move to leave the station.

The PCU uses value "a" when there is an odometer signal connected or when GPS is available. Otherwise it uses value "b".

Waypoints (WAYP)

This parameter can only be configured for data recording in DLX3 format.

Waypoints (WAYP) are necessary for subsequent trip analysis. Use the **Waypoints** parameter to define whether waypoints including trip data are recorded or not. Detailed information about waypoints is available in the "Format Specification DLX3 Rev. D". When the "auto" mode is set, the following procedure is used:

When the vehicle stops (stop/station, traffic light, etc.) a waypoint record is automatically generated by the PCU (format WAYP block type 1 in DLX3 archive).

While the vehicle is moving, the following rules are used for generating waypoints (Format WAYP block type 2 in DLX3 archive):

- When crossing the following speed values in up and down direction:
  25, 50, 75 100, 125, 150, … km/h
- Every 60 seconds since the last waypoint while the vehicle is moving with constant speed lower than 100 km/h
- Every 180 seconds since the last waypoint while the vehicle is moving with constant speed higher than 100 km/h

Additionally waypoints are recorded:

when the vehicle moves and covers a distance of 25 km from the last recorded waypoint (waypoint type 2)

when the PCU corrects the distance calculation, e.g. by recalibrating the odometer signal (waypoint type 2)

Door Level PET (Passenger Exchange Times)

This parameter can only be configured for data recording in DLX3 format.

Use this option to define if passenger exchange times should be recorded for every single door or not. If enabled, the following time values are recorded for each door and stop:

- When the first and the last passenger have passed the door
- When the door has been opened the first time at a stop
- When the door has been closed the last time at a stop

Note: The door contacts have to be hard wired at the digital inputs of the PCU so that passenger exchange times can be determined correctly. This allows detection of the status of the appropriate door (door signal).

Recording Profile

This parameter can only be configured for data recording in CSV format.

This parameter influences the structure of the CSV file, defines the separator between the columns and the character used as decimal point. This makes it easier to import data into a spreadsheet program and to compare data of several vehicles.

The parameter consists of key-value pairs separated by a comma. Missing key-value pairs will be replaced by their default value (see Table 45).

Key	Description
SEP:	Defines the characters for separation (column separator, decimal point). CP = Comma (C) as column separator; point (P) as decimal point (preferably for English file contents) SC = Semicolon (S) as column separator; comma (C) as decimal point (preferably for German or French file contents) Default: CP
DOORS:	Number of doors, for which columns must be created in the recording file Valid values: 1 to 192 (At least one door must be created.) Default: 10

	Note: When there are less doors defined than available in the vehicle, counting data of the remaining doors will not be recorded. In order to comfortably assembly CSV recording data of different vehicles of a fleet to one recording file in a spreadsheet program, all CSV recording files should have the same number of columns and the same format. Therefore choose a vehicle type of the fleet which has the most doors and use this number for all vehicles. Unnecessary columns in recording files of vehicles which have less doors will automatically remain empty. Make also sure to use the same separation.
PET:	The passenger exchange time (difference between the first time a passenger gets on and the last time a passenger gets off, in seconds) is determined for the stations and recorded during the final query at each station. Valid values are: 1 = function activated. 0 = function deactivated. Default: 0
QI:	Controls the recording of passenger information data (such as current station ID, line number, etc.) during the recording of an interim query. A = Passenger information data is recorded that was current at the time of arrival at the station. I = Passenger information data is recorded that is current at the time of the interim query. If these keys are not provided, then the default value 'A' is used.
QCI:	Controls the recording of passenger information data (such as the current station ID, line number, etc.) during the recording of a final query at a station (during departure) if an interim query was recorded beforehand. A = Passenger information data is recorded that was current at the time of arrival at the station. I = Passenger information data is recorded that was current at the time of the interim query. I = Passenger information data is recorded that is current at the time of departure from the station. If these keys are not provided, then the default value 'A' is used.
QC:	Controls the recording of passenger information data (such as the current station ID, line number, etc.) during the recording of a final query at a station (during departure) if no interim query was recorded beforehand. A = Passenger information data is recorded that was current at the time of arrival at the station. I = Passenger information data is recorded that is current at the time of departure from the station. If these keys are not provided, then the default value 'A' is used.

Table 39: Keys for the recording profile

Examples:

Key-value pair	Description
(empty)	Corresponds: SEP:CP,DOORS:10 Comma as column separator, point as decimal point, 10 columns for doors.
DOORS:12	Corresponds: SEP:CP, DOORS:12 Comma as column separator, point as decimal point, 12 columns for doors
SEP:SC	Corresponds: SEP:SC, DOORS:10 Semicolon as column separator, comma as decimal point, 10 columns for doors
SEP:SC,DOORS:12	Semicolon as column separator, comma as decimal point, 12 columns for doors
DOORS:15,SEP:SC	Semicolon as column separator, comma as decimal point, 15 columns for doors The sequence of key-value pairs is arbitrary.

Table 40: Examples for key-value pairs

Closing the Current Counting Data Recording File Manually

The PCU saves counting data in a recording file which is closed automatically after a configured time (**File Close Time**). You can force the PCU manually to close this file by clicking on the button **Close Rawdata File Now**.

CSV Viewer

This area is only available for data recording in CSV format.

The CSV Viewer gives an insight to the CSV recording file. Therefore click on **Get current CSV file**. You can follow how the counting system measures and records counting data.

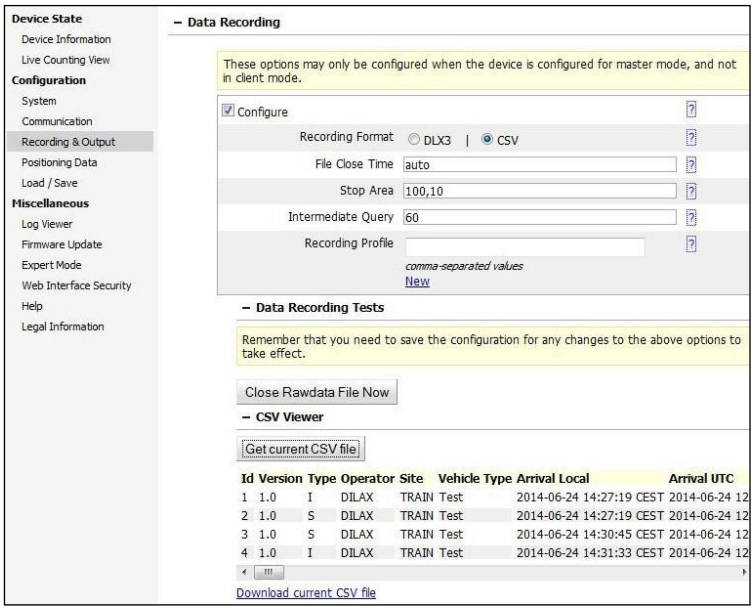


Figure 76: Display of the current CSV recording file

If you want to open the current CSV recording file in a spreadsheet program, click on **Download current CSV file** and save the file on your computer.

3.16.2 PCU usage in stationary applications (buildings)

For the usage in stationary applications, ensure the operation mode is set to **Master Mode with DCP Level 4** (**Operation Mode** parameter at **Configuration > System > General**, see chapter 3.5). In this mode, the XML format is used for data recording.

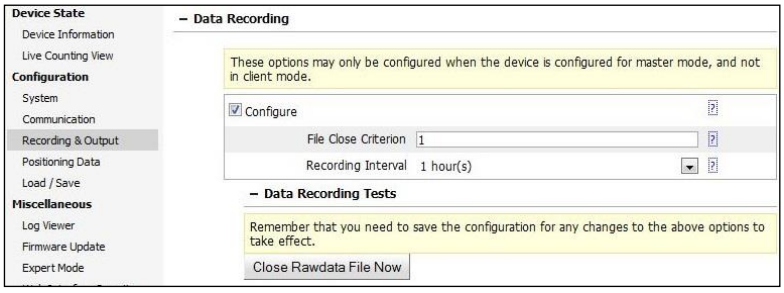


Figure 77: Configuration of data recording for a stationary system

Activate the **Configure** check box to record counting data.

If desired, change the default settings of **File Closing Criterion** and **Recording Interval**.

Parameter	Description	Default value
File Closing Criterion	Number of recording intervals which are concluded to one recording file.	1
Recording Interval	Duration of the recording interval.	1 hour(s)

Table 41: Default values for data recording in stationary systems

Closing the Current Counting Data Recording File Manually

The PCU saves counting data in a recording file which is closed automatically when a configured number of intervals are recorded (**File Closing Criterion**). You can force the PCU manually to close this file by clicking on the button **Close Rawdata File Now**.

3.17 Configuration > Recording & Output > Live Tracking

Use **Configuration > Recording & Output > Live Tracking** to activate and configure the live tracking function. This function can be used for several purposes, e.g. for vehicle tracking (GPS tracking), forwarding load information to wagon locator display systems at stations, for recognizing delays/early arrivals, etc.

This function generates tracking messages which will be sent to a server in the vehicle or at land side for further processing. Tracking messages contain information like vehicle name, current time and date, position of the vehicle, speed, driving state (at station, or driving), operational state (in operation or out of operation), and the state of the passenger counting system (in, out, door open, door closed). Each message describes the state of the vehicle at the time of message generation.

After generating a message, it can be sent via HTTP to a backend system. The backend system, e.g. a fleet management system, processes incoming messages of the PCU (storing or displaying data for GPS tracking). Details about the configuration of the data transfer via the DILAX real time protocol DRP (http, DCP Level 3) can be found in chapter 3.15.

Note: If there is no HTTP transmission configured or if the transmission fails, the PCU stores up to 100 tracking messages in a buffer using the first-in, first-out principle.

The PCU transfers the tracking messages via the internal WLAN/GSM/GPRS module (wireless interface). When there is no such module available, the Ethernet interface will be used for the transfer (transfer to a third party system in the vehicle). When it is not possible to transfer data, the oldest data records will continuously be overwritten.

You can decide if the tracking messages should contain live tracking data only or if the current load level of a consistent should be added to the live tracking data (see chapter 3.8). The definition of the parameters for tracking messages depends on the intended purpose.

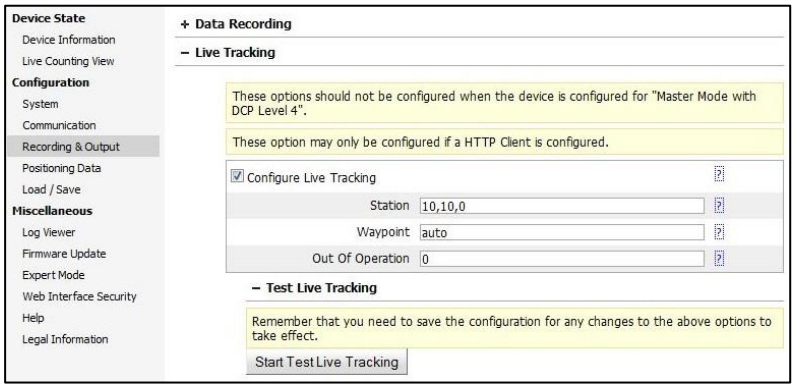


Figure 78: Configuration of live tracking

Activate the check box **Configure Live Tracking** to activate the generation of tracking messages. You can define message generation for the following situations:

- When the vehicle is standing at a station and leaving the station: **Station**
- When the vehicle moves to the next station and reaches the station: **Waypoint**
- When the vehicle is out of operation: **Out Of Operation**

Station

Enter a set of three parameters: **Length**, **Timeout**, and **Intermediate Query**. The parameters **Length** and **Timeout** control the detection of a station. The **Intermediate Query** parameter controls the generation of messages when the vehicle is standing at the station.

Parameter (Example)	Description
15,10,20	**Length:** Distance in meters the vehicle must move to leave the stop area. If the stop area has been left, a message with the stop summary is created. The example value defines a stop area of 15 meters.
15,**10**,20	**Timeout:** When no distance can be determined, leaving the station is alternatively determined by a time span. The vehicle must move at least for a specific time in seconds to leave the stop area. The example value defines a time span of 10 seconds.

15,10,**20**	**Intermediate Query:** Time period in seconds when messages are generated while the vehicle is standing at the station. The period starts when the vehicle reaches the station. The example value defines a period of 20 seconds.
15,10,**0**	**Intermediate Query:** No periodical messages are generated. In this case, only a summary message is generated when the vehicle leaves the station.
""(empty)	If you leave the field empty, no periodical message is generated while the vehicle is standing at the station, and no summary message is generated when the vehicle leaves the station.

Table 42: Parameters controlling the generation of live tracking messages at a station

Waypoint

You can control the generation of messages while the vehicle is moving to the next station and when it reaches a station.

Parameter (Example)	Description
auto	Messages will automatically be generated depending on the speed of the vehicle. To determine when a message has to be generated, the PCU uses the following procedure: 1. When crossing the following speed values in up and down direction: 25, 50, 75 100, 125, 150,…. km/h 2. Every 60 seconds since the last message trigger while moving with constant speed lower than 100 km/h 3. Every 180 seconds since the last message trigger while moving with constant speed higher than 100 km/h 4. When the vehicle stops (stop/station, traffic light, etc.).
30	Time period in seconds. Messages are generated periodically independent from the speed. Additionally, a message will be generated, when a station is reached. The example value defines a period of 30 seconds.
""(empty)	If you leave the field empty, no messages will be generated when the vehicle moves to the next station or reaches a station.

Table 43: Parameter controlling the generation of live tracking messages when the vehicle moves to the next station

Out Of Operation

You can control the generation of messages while the vehicle is out of operation. With this parameter you can reduce the number of messages generated for this operational state, or you can suppress the generation completely.

Parameter (Example)	Description
300	Time period in seconds. Messages are generated periodically. The example value defines a period of 300 seconds.
0	No messages are generated when the vehicle is out of operation.

Table 44: Parameter controlling the generation of live tracking messages when the vehicle is out of operation

Test Live Tracking

To test the live tracking function you can generate a message manually. Press the button **Start Testing Live Tracking**. The PCU generates a tracking message according to the current situation (at station, or moving). When the HTTP transfer is enabled, the message will be sent automatically.

Note: Live tracking is commonly done with using a GSM (GPRS) connection. If you want to follow the vehicles track even when it is moving to the next station, you should select a **Permanent GPRS connection** at **Dial-on-Demand Routing** in the GSM configuration (see chapter 3.11). Select the **Dial-on demand** setting when only station summary should be transferred.

Notice: The live diagnostics function underwent a fundamental change from Version 1.26.0. Therefore, live tracking and live diagnostics configured in an earlier version have to be new configured (**Configuration > Recording & Output > Live Tracking** and **Configuration > Recording & Output > Live Diagnostics**) as described in this product manual.

3.18 Configuration > Recording & Output > Live Diagnostics

Live diagnostics can be activated and configured via Configuration > Recording & Output > Live Diagnostics**.** This function allows the diagnostics state of a count system to be tracked in real time.

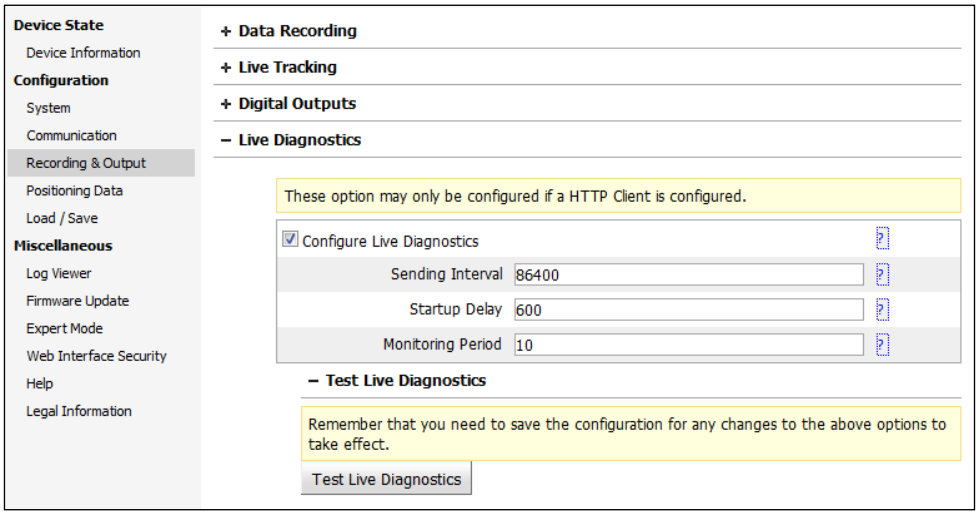


Figure 79: Configuration of Live diagnostics

After live diagnostics has been activated, the PCU generates messages with diagnostics information about errors detected by the PCU. These messages are sent to the configured background system via http (see 3.15).

Notice: Make sure that the master PCU receives the diagnostics information. Activate the **system monitor** parameter in the **Remote information services** for all configured Client PCUs (see 3.19.3.3).

Live diagnostics is controlled via three parameters: **Send interval, Start delay** and **Check interval.**

Send Interval

Parameter (example)	Description

86400	A status message is generated every 86400 seconds (one day). As a result, the background system receives the count system status on a regular basis, even if the error status has not changed. The value range is between 600 (ten minutes) and 86400 seconds (one day). The default value is 86400 seconds.

Table 45: Send interval parameter for live diagnostics

Start delay

Parameter (example)	Description
600	After switch-on or a restart, the count system waits 600 seconds (10 minutes) for the system status check (error diagnostics) to start. During this time, the vehicle should be ready for operation. Possible values are between 180 seconds and 3600 seconds (1 hour).

Table 46: Start delay parameter for live diagnostics

Check interval

Parameter (example)	Description
10	The count system checks its status every 10 seconds after the **start delay** has finished. If the status changes because an error has been detected, for example, a status message is generated. The value range is between 3 and 10 seconds. The default value is 10 seconds.

Table 47: Check interval parameter for live diagnostics

Testing live diagnostics

To test the live diagnostics function, you can generate status messages manually. Click the on the **Test live diagnostics** button. The PCU generates a status message depending on the current situation (error status). If HTTP transfer is activated, the message will be sent automatically.

Notice: The live diagnostics function is normally used with a GSM (GPRS) connection. If you want to track the vehicle's position, activate **Permanent GPRS connection** with **Dial-on-Demand-Routing** in the GSM configuration (see Section 3.11). Select **Dial-on demand** if you want to track only the changes to the diagnostic status.

Notice: The live diagnostics function underwent a fundamental change from Version 1.26.0. Therefore, live tracking and live diagnostics configured in an earlier version have to be new configured (**Configuration > Recording & Output > Live Tracking** and **Configuration > Recording & Output > Live Diagnostics**) as described in this product manual.

3.19 Configuration > System > Clients

A master PCU can control up to 31 client PCUs. If the PCU you configure acts as a master PCU the management of its client PCUs is configured by using the page **Configuration > System > Clients**.

3.19.1 Common Description of the Configuration of Clients

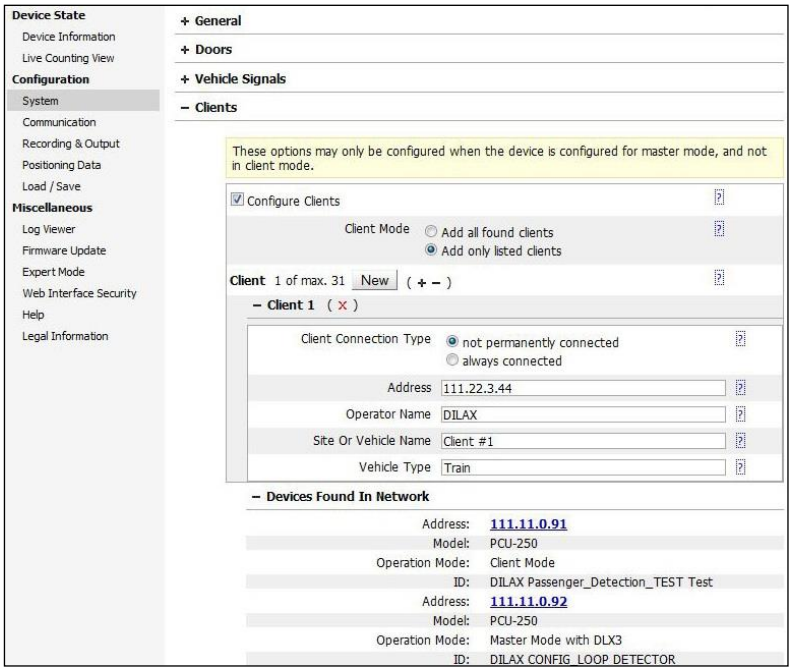


Figure 80: Configuration of the client PCUs managed by a master device

Enabling Client Configuration

When a PCU operates in master mode additional client PCUs can extend the counting system. Activate the check box **Configure Clients** to activate this system extension.

Note: If the live tracking diagnostics functionality should be used (Configuration > Recording & Output > Live Tracking, see 3.17), you have to use the fix client configuration.

Automatic Detection of Client PCUs in the Network

To simplify the configuration, a master PCU automatically detects all client PCUs which are connected to the same local Ethernet network. Therefore there are two methods available. Choose one option at **Client Discovery Method**:

rARP: Default method for detecting client PCUs in the same local Ethernet network. If no automatic detection is required, keep this option selected.

By IP only: When the rARP method is not supported or not permitted, choose the **By IP only** method. The following conditions must be fulfilled in order to have a successful detection via IP:

- The clients must have a fixed IP address.
- The clients must be permanently connected.

Note: The **By IP only** method is not suitable for the following situations:

5. Variable train configurations,
6. Client PCUs connected via DHCP,

7. Usage of DHP Level 1.

You can display the detected client PCUs in the lower part of the configuration page. Therefore open the **Devices Found In Network** area.

Note: For every device found, an address is displayed. When you click on this hyperlink, a new browser window will open containing the web interface of this device.

Fix Client Configuration

If the master PCU should be connected to a fix set of client PCUs, a list of all client PCUs must be created:

1. Select "Add only listed clients" at **Client Mode**.
2. Add a new client PCU by pressing the **New** button.
3. Select how the client PCU is connected to the master PCU (**Client Connection Type**):
   "not permanently connected" (e.g. train length can be extended or reduced but always with the same set of wagons) or "always connected" (e.g. in a bus).

   Note: If you select "not permanently connected", the master PCU will not produce an error message when the communication between the master PCU and the client PCU is interrupted.

   Enter at least one unique identification property of the client PCU:

   - **Address**
   - **Operator Name**
   - **Site Or Vehicle Name**
   - **Vehicle Type**

   Note: The combination of these properties must form a unique identifier of the client PCU. If the **Address** is set to **DHCP**, at least one of the other three properties must be specified and unique for the client in the network. An empty field works like a wildcard where any value of this client property matches the identifier. Enter values into all fields (**Operator Name**, **Site Or Vehicle Name**, **Vehicle Type**) to avoid identification problems, e.g. when detecting clients or single doors.

Note: If the live tracking diagnostics functionality should be used (Configuration > Recording & Output > Live Tracking, see 3.17), the **Client Connection Type** must be set to "always connected" and the parameters **Operator Name**, **Site Or Vehicle Name**, and **Vehicle Type** must be defined.

Variable Train Assembly

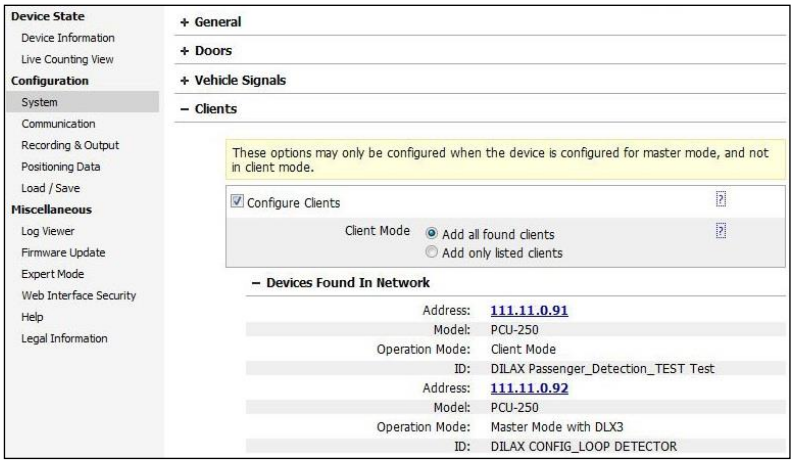


Figure 81: Configuration of client PCU detection for a variable train assembly

If there is one master PCU in the traction vehicle and client PCUs in the wagons, a train can be assembled in a way unpredictable for the master PCU. In this case each client the master PCU ever detects will be managed by the master PCU. The list of connected PCUs is dynamically updated. To configure this case select "Add all found clients" at **Client Mode** (see Figure 88):

Note: If the communication between the master PCU and a client PCU is interrupted the master PCU assumes the corresponding wagon is removed from train. No error messages will be generated.

Remote Information Provider

If project-specific circumstances do not allow that the master PCU executes all master functionalities, then individual functionalities may be passed to client PCUs in consultation with the DILAX customer service.

Detailed information can be found in chapter 3.19.3.

3.19.2 DCP Level 1 Client Configuration

When the clients are connected to an RS485 network via DCP Level 1 protocol, the client configuration is slightly different from the common configuration.

Note: In contrast to the common client detection, DCP Level 1 only supports a fix set of client PCUs. This is because client PCUs cannot be dynamically added to or removed from an RS485 bus.

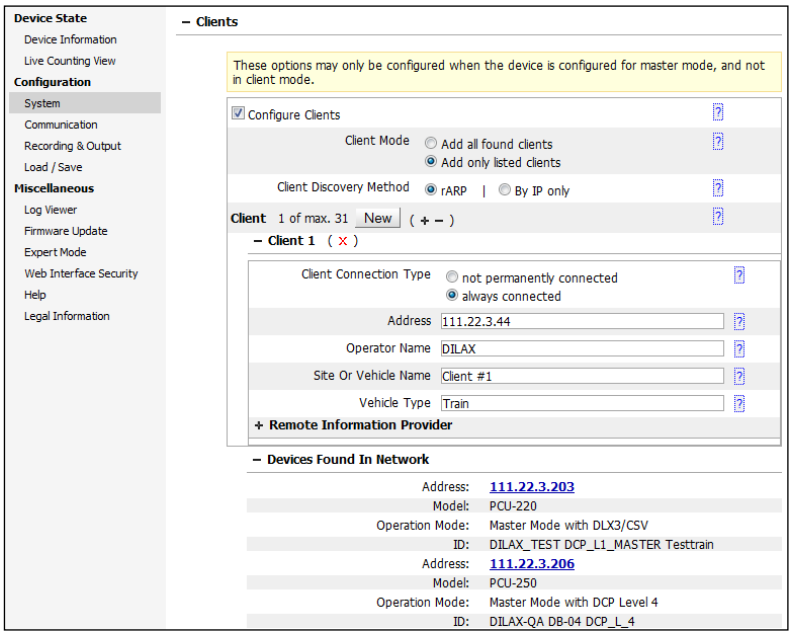


Figure 82: Client configuration with a DCP Level 1 network

Follow these steps to configure a DCP Level 1 network:

1. Connect all client PCUs and the master PCU to the RS485 bus.
2. Switch all devices on.
3. First configure the clients:
   For each client, open the **Configuration > Communication > Comm. Protocols** page and select **DCP Level 1** as **Protocol**. Set a **DCP Level 1 address** as client address (client 1…client 16) which must be unique for the RS485 bus.
4. Reset the clients.
5. At the master PCU, open the Configuration > Communication > Comm. Protocols page and select DCP Level 1 as Protocol. Set a DCP Level 1 address to Master and save the configuration.
6. Open the Configuration > System > Clients page and select the appropriate Client Discovery Method. The Clients Found In Network list shows the clients.
7. Activate the check box **Configure Clients**.
8. Select Add only listed clients for the Client Mode.
9. Press the **New** button to add a new client.
10. Select always connected in the Client Connection Type.
11. Enter the DCP Level 1 Client address (e.g. "Client 3") in the **Address** field.
12. The fields Operator Name, Site Or Vehicle Name, and Vehicle Type remain empty.

Note: Settings in the **Remote Information Provider** section are not supported when DCP level 1 protocol is used. Please do not configure them.

13. Repeat steps 9 to 12 for each DCP Level 1 client.
14. Save the configuration.

3.19.3 Using the Remote Information Provider Function

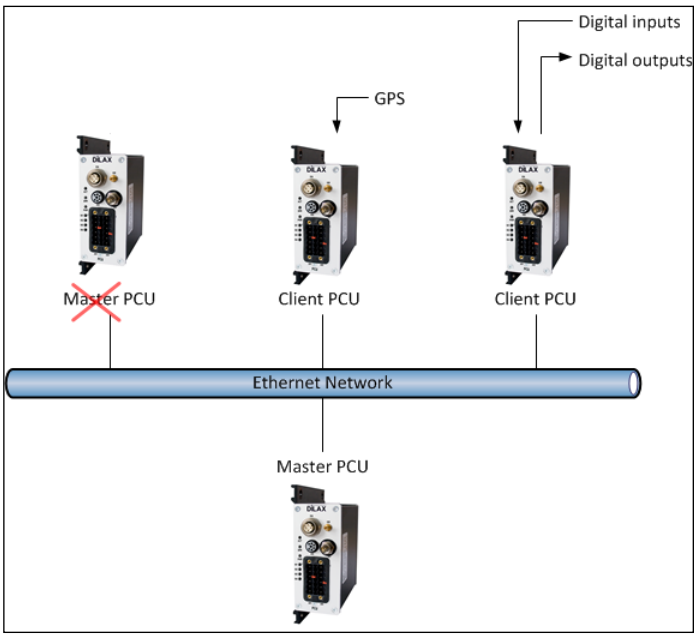


Figure 83: Master PCU using master functionality provided by client PCUs

If project-specific circumstances do not allow that the master PCU executes all master functionalities, then individual functionalities may be passed to client PCUs in consultation with the DILAX customer service.

Client PCUs must run in operation mode "client mode" (web interface of client PCU, **Configuration > System > General**, see chapter 3.5).

Client PCUs should always be connected to the master PCU (web interface of master PCU, **Configuration > System > Clients**, **Client Connection Type** "always connected", see chapter 3.18.1.

Note: Only use this function when you know in detail which information can be provided by the appropriate client PCU. This avoids misconfigurations.

The Remote Information Provider function can only be set on a master PCU. Settings defined in this function can only be applied at runtime to the appropriate client PCU. Only time-uncritical settings are possible.

Settings are stored on the master PCU and not on the client PCUs. After restarting a client PCU the device will use its originally stored configuration. As soon as the master PCU recognizes that the appropriate client PCU is available again, it will resend the remote information provider settings to carry on receiving information.

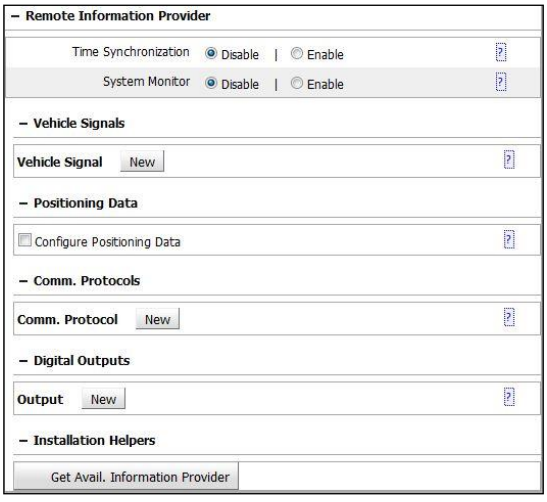


Figure 84: Remote information provider

Proceed as follows to send settings to a client PCU and receive information from this device:

1. Select the appropriate client PCU or create a new client.
2. Display available information provided by the client PCU (**Installation Helpers**, see chapter 3.19.3.1).
3. Adjust which information should be used from the client PCU (**Time Synchronization**, **System Monitor**, **Vehicle Signals**, **Positioning Data**, **Comm. Protocols** and **Digital Outputs**; see chapters 3.19.3.2 to1).
4. Save the configuration of the master PCU.

3.19.3.1 Remote Information Provider > Installation Helpers

Use this function to display which hardware is connected to the client PCU. On this basis, you can afterwards define remote information provider settings.

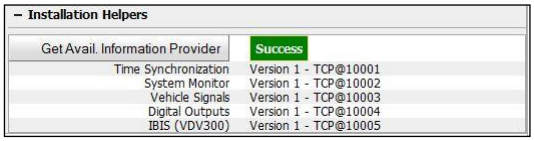


Figure 85: Installation helpers for remote information provider

Click the **Get Avail. Information Provider** button to show information.

If no information is displayed, make sure that the following is fulfilled before clicking the button again:

- The client PCU has been configured as client and not as master.
- A firmware version 1.18.0 or higher is running on the client PCU.
- There is an Ethernet connection between the master PCU and the client PCU.

3.19.3.2 Synchronizing the System Time of the Master PCU with the System Time of the Client PCU

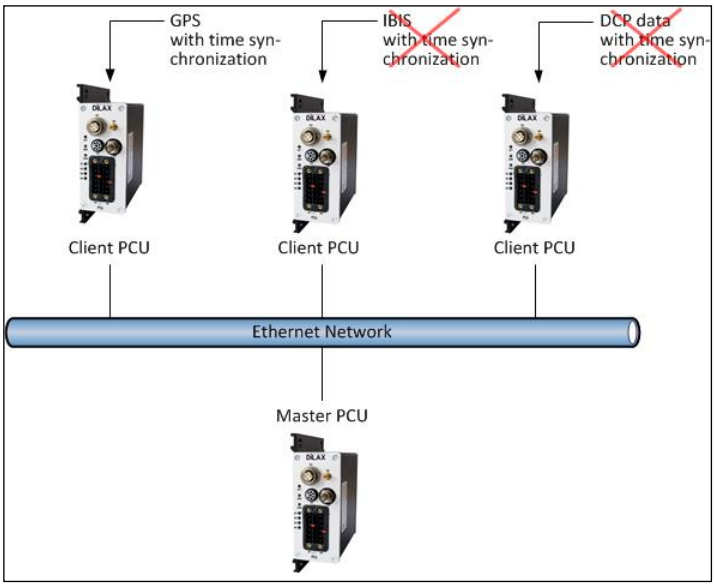


Figure 86: Only one client PCU may be used for time synchronization

The system clock of the PCU can be synchronized with different reference time sources (see chapter 4.1).

Note: Synchronizing the system time with a client PCU is only possible, when the client PCU itself executes a time synchronization.

The master PCU can synchronize its time only with one source in the counting system.

Always prefer time synchronization with a source which is directly connected to the master PCU. Only use a client PCU for this functionality, if there is no other possibility.

The Remote Information Provider functions offers three possibilities for time synchronization:

By activating the **Time Synchronization** option:

Figure 87: Time synchronization via remote information provider

By enabling the **Time Synchronization** option the time of the master PCU will be synchronized with the time of the appropriate client PCU.

Via positioning data: See chapter 3.19.3.5 for details.

Via IBIS (VDV300) communication protocol: See chapter 3.19.3.6.1 for details.

3.19.3.3 Receiving Diagnostic Data from the Client PCU

By enabling the **System Monitor** option the master PCU can retrieve diagnostic data from the client PCU. This includes:

- Status of the configuration
- Status of the device
- Status of the SST-100 (if available)

Errors in diagnostic data are written to the system log.

3.19.3.4 Remote Information Provider > Vehicle Signals

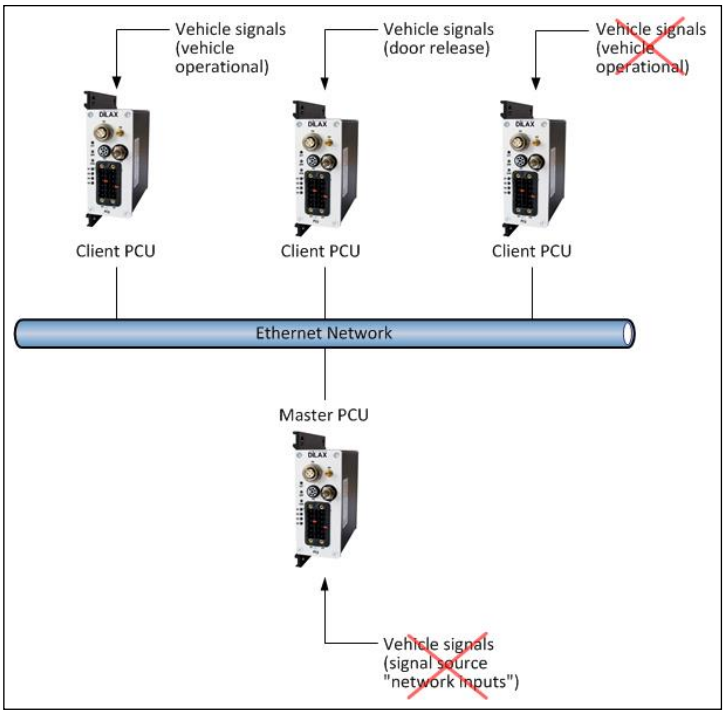


Figure 88: Receiving vehicle signals via client PCUs

When client PCUs support vehicle signals at its digital inputs, you can define signals which the master PCU should receive from a client PCU below **Remote Information Provider > Vehicle Signals**.

Note: When there are vehicle signals defined in the master PCU (**Configuration > System > Vehicle Signals**) and the **Signal Source** "Network Inputs" is chosen, then the master PCU cannot receive vehicle signals from a client PCU.

Each vehicle signal may only be provided by one client PCU.

Defining General Input Types

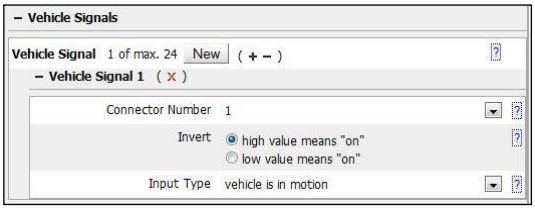


Figure 89: Setting vehicle signals at remote information provider

General input types are:

- Vehicle is in motion
- Door release, left side
- Door release, right side
- Vehicle operational
- Vehicle at regular stop

1. Click the **New** button to create a new vehicle signal.
2. Define the input source:
   – The signal source is always the digital input of the client PCU. Select the **Connector Number** (this is the input number INx and not the PIN number Xnn).

Note: Each input source can only be chosen once per counting system. When defining several vehicle signals, choose a different **Connector Number** for each vehicle signal.

The chosen vehicle signal must be connected to the appropriate digital input of the client PCU. It is not possible to use digital inputs which are connected to the INP-450.

Ensure that the vehicle signals of master PCU and client PCU are not set twice.

3. Select the vehicle signal connected the digital input in the **Input Type** list.
4. Set the **Invert** behavior (Standard: high value means "on" = not inverted).

Defining the Input Type Event

The master PCU can be configured to raise events when the states of digital inputs change at the client PCU.

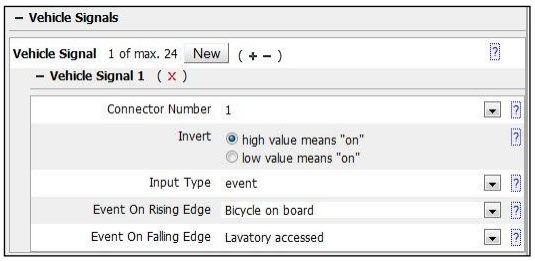


Figure 90: Event generation at remote information provider

1. Click on the **New** button to create a new vehicle signal.
2. Define the input source:
   - The signal source is always the digital input of the client PCU. Select the **Connector Number** (this is the input number INx and not the PIN number Xnn).

Note: Each input source can only be chosen once. When defining several vehicle signals, choose a different **Connector Number** for each vehicle signal.

The chosen vehicle signal must be connected to the appropriate digital input of the client PCU. It is not possible to use digital inputs which are connected to the INP-450.

Ensure that the vehicle signals of master PCU and client PCU are not set twice.

3. Select the entry "event" from the **Input Type** list.
4. Select an event in the lists **Event On Rising Edge** (input state goes from low to high) and **Event On Falling Edge** (input state goes from high to low).

   Typically there are pairs of events, e.g. "Wheelchair on board" and "Wheelchair unload". If you want to register both events, select one event for the rising and the other for the falling edge.

   If you only want to register one event, select this event in the proper list and select "No event" in the other one.

Note: If vehicle signals are used through the remote information services, then you **cannot use any vehicle signals** via the **network inputs** (**Configuration > System > Vehicle Signals** and **'network input'** as **Signal Source**). Furthermore, no **passenger information data** and no **position data** will be received via network with the DILAX Counting Protocol (see Chapter 6.2.2).

3.19.3.5 Remote Information Provider > Positioning Data

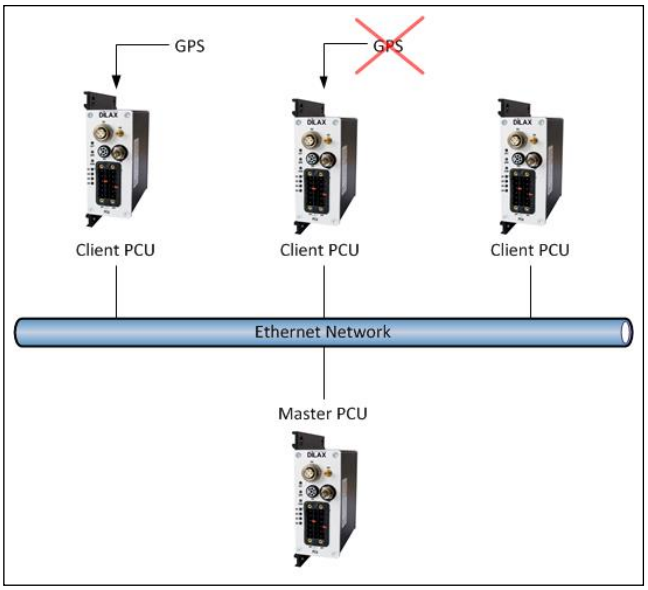


Figure 91: Only one client PCU may supply GPS information

The master PCU can be configured to receive the sampling of the position via the internal receiver of the client PCU.

Note: GPS information may only be received by the master PCU from one client PCU.

When the client PCU is equipped with an internal GPS receiver (e.g. Navstar, Glonass) the system can receive positioning and time data directly from the satellite-based positioning system. Therefore activate the **Configure Positioning Data** check box.

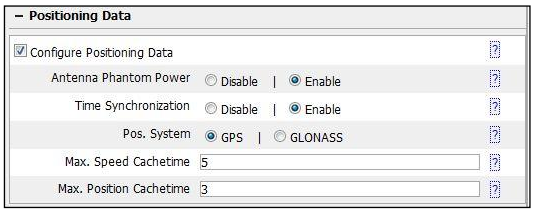


Figure 92: Event generation at remote information provider

For active GPS antennas enable **Antenna Phantom Power**. This supplies the signal amplifier of the antenna with the required power via the antenna cable. When this option is not activated the GPS reception may be incorrect or insufficient.

The system clock of the PCU can be synchronized with different reference time sources (see chapter 4.1). By enabling the **Time Synchronization** option, the time of the master PCU will be synchronized with the time of the appropriate client PCU. The coordinates of the current position are recorded in WGS84 format.

Note: The master PCU can synchronize its time only with one source in the counting system.

When the client PCU is equipped with an internal GPS module which supports both, the American NAVSTAR as well as the Russian GLONASS navigation system (see 2.4.7), the type of the navigation system can be selected at **Pos. System**. The GPS receiver will then be switched into the working mode of the chosen system.

Note: If GLONASS is chosen data is only taken from GLONASS positioning system, which may affect the time to first fix (TTFF).

The positioning system can only be chosen at one client PCU, not several.

Situations with GPS failure

There may be receiving problems between the client PCU and GPS in certain situations, e.g. when the vehicle is in an area where no GPS reception is available (shielded factory hall, driving through tunnels, underpasses and/or bridges).

Last valid positioning data which the system has sent within a specific time is stored in the cache. In case of a connection failure the client PCU receives data directly from the cache memory. The maximum times for buffering the last GPS coordinates and the last velocity value (calculated by the client PCU) in the cache memory can be configured.

Max. Speed Cachetime
Maximum time in seconds for buffering a velocity value
Range of values: [0...900 s], Default: 5 s

Max. Position Cachetime
Maximum time in seconds for buffering GPS coordinates
Range of values: [0...30 s], Default: 5 s

Correct time values for buffering decisively influence the quality of the recorded data. Usually, the calculation of distance values is done via tachometer or odometer signal. When this signal is not available, the client PCU calculates distance values on the basis of GPS data and uses the buffered values from the cache in case of a connection failure. When buffered values are too small or when there is no valid data, a calculation will not be possible.

With these parameters, the number of recorded way points with invalid positioning data (marked by "n/a" in recording data) can be minimized (see 3.16.1 for details about way points). In the majority of cases the default values are sufficient. Optimal values for buffering times depend on operating conditions of the vehicles (line management, etc.) and can only be determined by empirical tests.

3.19.3.6 Remote Information Provider > Comm. Protocols

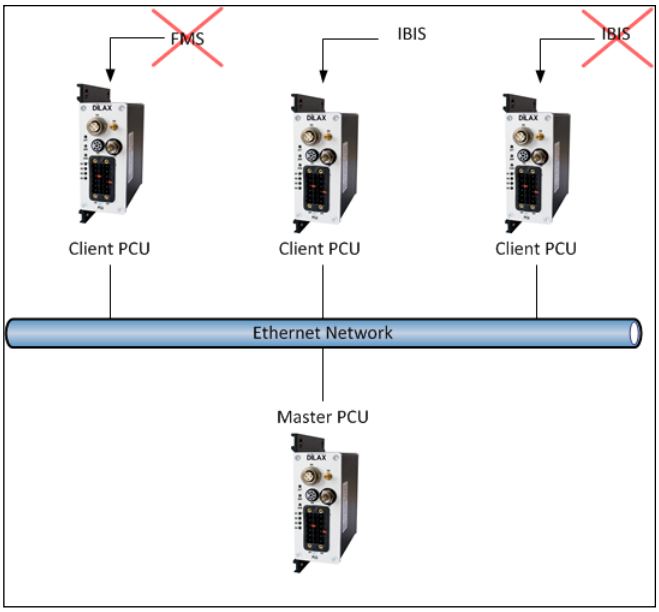


Figure 93: Only one client PCU may supply a specific communication protocol

The master PCU can receive additional information provided by the onboard unit via the client PCU. Therefore the client PCU communicates via different protocols with the onboard unit.

Note: One communication protocol may only be supported by one PCU in the counting system.

3.19.3.6.1 IBIS (VDV300) Protocol

The client PCU might support the IBIS protocol which allows the client PCU to record driving information (e.g. line number, station identification, and station name) provided by an onboard unit which works as an IBIS master. The information is encoded according to the VDV300 standard. Additionally, the system date and time of the client PCU can be synchronized with the vehicle time provided by the IBIS master.

Recorded VDV300 telegrams are defined as a comma separated list. The telegram notation of the VDV300 standard is used for the telegram definition (see VDV300 specification for detailed information about the notation).

Example: kZZ,zPZZZ,zZZZZZ,nBHHHHH,zIHC,xZZZZ

Note: The station name display text "zIHC" is a telegram with a variable number of characters 'C'. Instead of writing a ‘C’ for each character only the first character must be defined. This simplifies the configuration of this common used telegram.

If the IBIS (VDV300) protocol is selected, VDV300 data is received via a serial interface (baud rate is 1200 bps, 7 data bit, even parity bit and two stop bits). For the connection of the IBIS bus see chapter 2.4.9.

Configuring an IBIS protocol

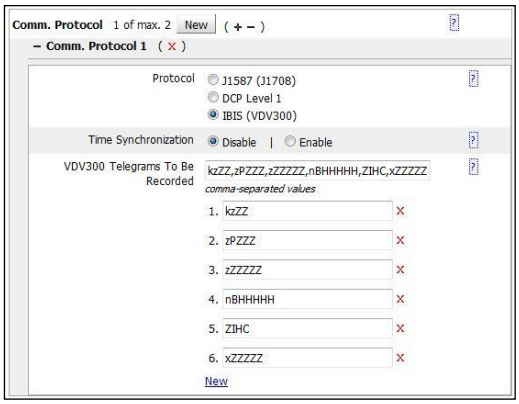


Figure 94: Configuration of the IBIS (VDV300) protocol vial remote information provider

Proceed as follows to make settings for the client PCU:

1. Press the **New** button next to **Comm. Protocol** to create a new protocol profile for the client PCU.
2. Select "IBIS (VDV300)" as **Protocol** for the communication between client PCU and onboard unit.
3. Select a **Time Synchronization** option for synchronizing the time of the client PCU.
4. Enter the list of VDV300 telegrams to be recorded. Alternatively, use **New** to enter each element into a separate input field.

3.19.3.7 Remote Information Provider > Digital Outputs

With this function, a client PCU instead of the master PCU will signalize error signals of the counting system to the onboard unit. The appropriate client PCU must have digital outputs (see also chapter 2.4.9) and must be connected to the onboard unit.

Note: A client PCU can only signalize error signals to the onboard unit. A master PCU which is equipped with digital outputs and is connected to the onboard unit, can additionally signalize the occurrence of passenger detection events and counting impulses for boardings and alightings (see chapter 3.22).

When the error state vanishes, the error state signal will be released automatically. Between the occurrence of an error state change and the change of the error signal at the digital output a maximum delay of 20s can occur.

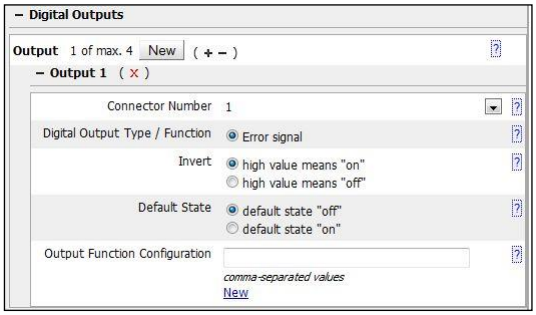
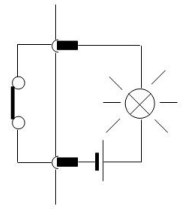
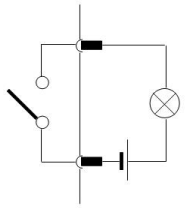


Figure 95: Configuring digital outputs via remote information provider

Proceed as follows to use digital outputs of a client PCU:

1. Press the **New** button to define a digital output of the client PCU.
2. Select the **Connector Number** (see chapter 2.4.9.2 for the connector names).
3. Only **Error signal** is available as **Digital Output Type / Function**.
4. Select the **Invert** behavior of the digital output depending on the logic of the device consuming the digital output signal:

Invert: High value means "on"	
Logical Signal	Electrical Signal
on	
off	

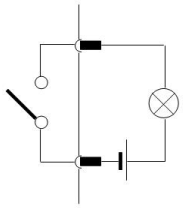
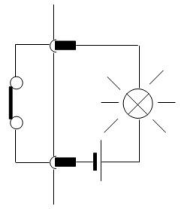
Invert: High value means "off"	
Logical Signal	Electrical Signal
on	
off	

Table 48: Inversion behavior of digital output

5. Select the **Default State**. This is the logical state the digital output is set when:

- The system starts after power on or reboot.
- The digital output is configured the first time or the configuration changes.
- An error state of the digital output function is detected (secure state).

The error signal function does not require an entry in the **Output Function Configuration** field. This field can be left empty.

3.20 Configuration > Communication > Wi-Fi

On the page **Configuration > Communication > Wi-Fi** the Wi-Fi settings of the PCU can be configured.

Note: This menu is only visible if the PCU is equipped with an internal Wi-Fi communication module.

Adding a Wi-Fi Network

To activate the Wi-Fi operation of the PCU, add the settings of all Wi-Fi networks the PCU should be assigned to.

Note: You can configure up to **five Wi-Fi networks**. Each must be identified by a unique Wi-Fi network name (SSID). The PCU connects to the best available network it can find. Once the connection to a network is lost, the PCU automatically starts to search for another available network from the list of configured networks and connects to it.

Proceed as follows:

1. Press the button **New** to create a new set of settings of a Wi-Fi network.
2. Enter the **Wi-Fi Network Name (SSID)**.
3. Select the **Encryption Protocol**.

   The following encryption types are supported:

   - WPA2 Personal (IEEE 802.11i-2004)
   - WPA Personal (IEEE 802.11i)
   - WEP (IEEE 802.11)
   - No encryption

Note: If you select the **WEP** encryption protocol, the **Pre-shared Key** is restricted to one of the following values:

6. A 5 character value (for 64-bit encryption).
7. A 13 character value (for 128-bit encryption).
8. A 10 hexadecimal-character value like A1F35DBF77 (for 64-bit encryption).
9. A 26 hexadecimal character value like 22A6C112FDA80F247903ACF0D3 (for 128-bit encryption).

4. Enter the **Pre-shared Key**.

Automatic Wi-Fi Network Configuration (DHCP)

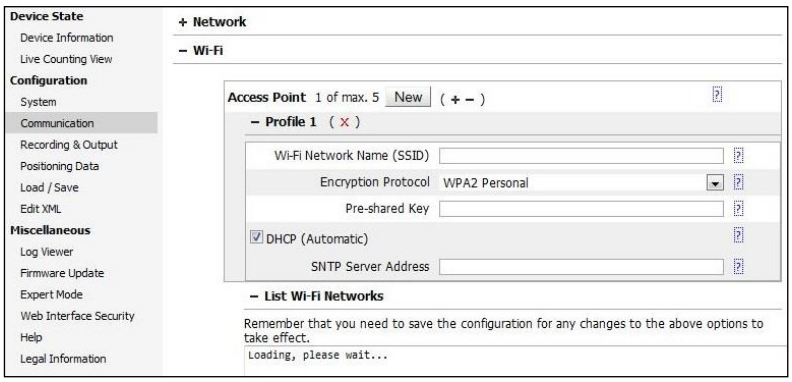


Figure 96: Automatic configuration of the Wi-Fi network interface

If the Wi-Fi network to be used contains a DHCP server (as most access points have), use the automatic configuration:

1. Activate the check box **DHCP (Automatic)**. This will set the IP configuration of the Wi-Fi network interface automatically (see Figure 106).
2. In the **Device Hostname** input field you can define a hostname for the device. This is an optional input. It is used in the DHCP protocol to signalize the DHCP server which device is requesting an IP address.
3. If you want to synchronize the system date with a time server (SNTP), enter "auto" into the **SNTP Server Address** input field. Otherwise, leave this field empty to disable time synchronization via Wi-Fi or manually enter a known IP address.

Note: The internal WLAN module of the PCU supports WLAN standards 802.11 a, b, and g. This allows using WLAN networks with 2,4 GHz and 5 GHz. Please consider legal framework for the usage of WLAN (e.g. in Europe, the usage of WLAN networks with 5 GHz in outdoor area is normally not allowed).

Manual Wi-Fi Network Configuration

If there is no DHCP server in the Wi-Fi network you must configure the network interface manually:

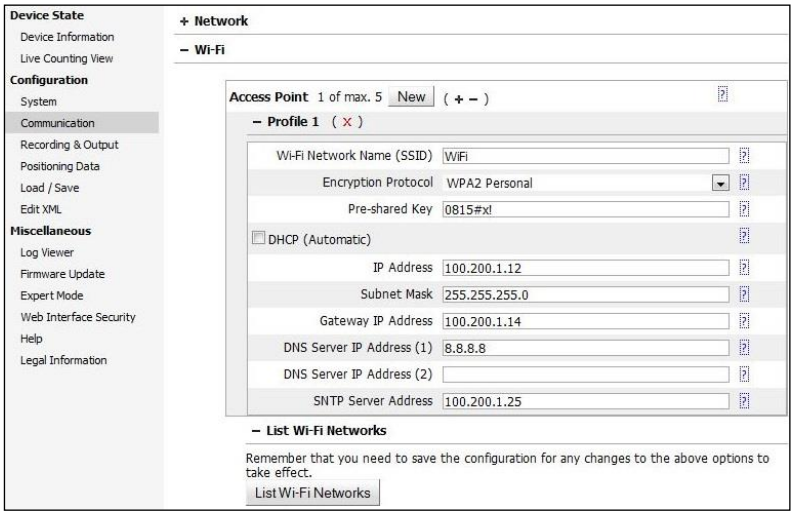


Figure 97: Manual configuration of the Wi-Fi network interface

1. Deactivate the check box **DHCP (Automatic)**.
2. Enter the **IP Address**.
3. Enter a **Subnet Mask**.
4. Enter the **Gateway IP Address** if you require access to another network (e.g. the internet).
5. Enter the **DNS Server IP Address (1)** if you want to configure the FTP host name in the FTP server & client configuration (see chapter 3.12) as domain name notation.
6. If necessary, you can enter an additional, second DNS server address.
7. Enter a known time server IP address into the **SNTP Server Address** input field to synchronize the PCU with a time server or leave the field empty if the time synchronization via Wi-Fi should be disabled.

Configuration of the Time Server (SNTP)

A time server is used to synchronize the system time with a time reference (see chapter 4.1 for clock synchronization). The time server delivers the current time to the PCU. It can be set automatically by the DHCP server if the corresponding field is set to auto or manually, using this dialog.

Note: Some DHCP servers do not deliver the address of an SNTP server. In this case, the SNTP server has to be specified manually even if all other IP settings are gathered automatically.

The PCU is not a router. The network adapters of the Ethernet interface (IP address of PCU and WLAN interface) have to be configured in a way that they are not located within an identical network segment. Example:

Network adapter of PCU (ETH):	192.168.23.200
Network WLAN:	192.168.24.200
Subnet mask:	255.255.255.00

3.21 Configuration > Communication > Comm. Protocols

The PCU can communicate with the onboard computer via different protocols. This allows to control and monitor the PCU or to receive additional information provided by the onboard unit.

3.21.1 J1708/J1587 Protocol

The J1708 bus interface and the J1587 protocol is supported by the PCU. This allows the PCU to be easily integrated into onboard units of vehicles that communicate via J1708.

One PCU can only support three doors for people counting (restriction by the J1708/J1587 specification). But the counting system can be extended by additional PCU devices so that it is possible to monitor up to nine doors.

Open the page **Configuration > Communication > Comm. Protocols** to activate the J1708/J1587 interface.

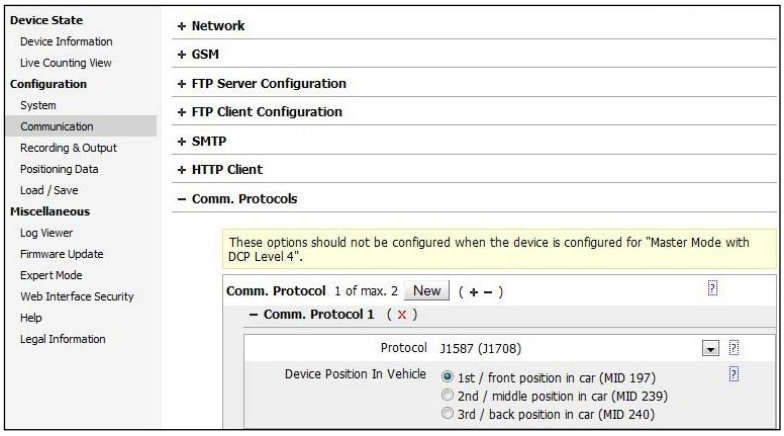


Figure 98: Configuration of the J1708/J1587 communication protocol

1. Click the **New** button to create a protocol profile.
2. Select the **Protocol** "J1587 (J1708)".
3. Select the position where the PCU is installed at **Device Position In Vehicle**. The onboard computer of the vehicle uses this information to request the correct PCU.

Note: When the **Profile** field does not contain a string (default setting), the PCU counts events only up to a value of 255. Further events will not be registered until the value is explicitly reset to 0 (zero) by the board computer. If the PCU should automatically reset the value to 0 when the value 255 is reached, enter the string "DELTACOUNT" into the **Profile** field.

3.21.2 IBIS (VDV300) Protocol

The PCU supports the IBIS protocol which allows the PCU to record driving information (e.g. line number, station identification, and station name) provided by an onboard unit which works as an IBIS master. The information is encoded according to the VDV300 standard. Additionally, the system date and time of the PCU can be synchronized with the vehicle time provided by the IBIS master.

Note: To record VDV300 telegrams, Master Mode with DLX3 (see chapter 3.5) must be activated.
Otherwise, the PCU acts as door client (see chapter 3.21.3).

Note: To record VDV300 telegrams, data recording must be activated (see chapter 3.16).
A telegram is recorded at the first time the PCU receives it and on every time the content of the telegram changes.

Recorded VDV300 telegrams are defined as a comma separated list. The telegram notation of the VDV300 standard is used for the telegram definition (see VDV300 specification for detailed information about the notation).

Example: kZZ,zPZZZ,zZZZZZ,nBHHHHH,zIHC,xZZZZ

Note: The station name display text "zIHC" is a telegram with a variable number of characters 'C'. Instead of writing a 'C' for each character only the first character must be defined. This simplifies the configuration of this common used telegram.

If the IBIS (VDV300) protocol is selected, VDV300 data is received via a serial interface (baud rate is 1200 bps, 7 data bit, even parity bit and two stop bits). For the connection of the IBIS bus see chapter 2.4.9.

Configuring an IBIS protocol

Open the **Configuration > Communication > Comm. Protocols** page to activate the IBIS (VDV300) interface.

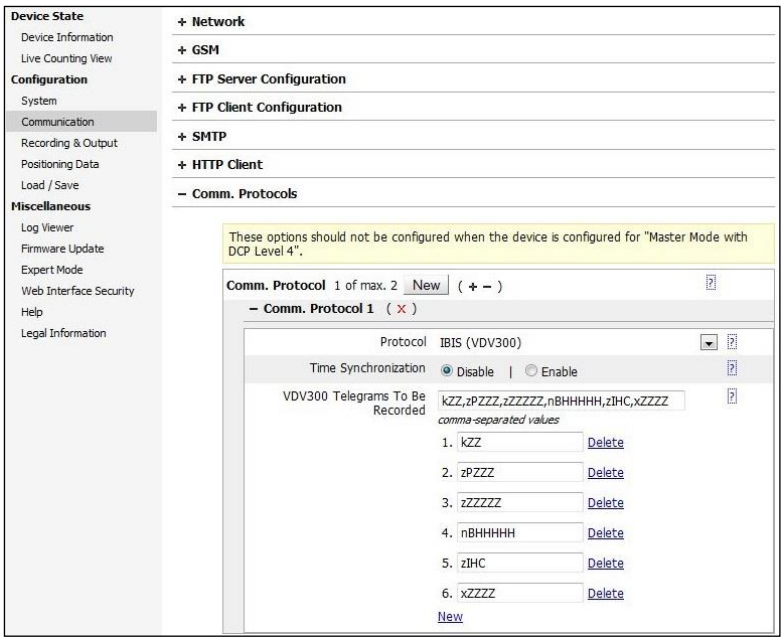


Figure 99: Configuration of the IBIS (VDV300) protocol

1. Press the **New** button next to **Comm. Protocol** to create a protocol profile.
2. Select "IBIS (VDV300)" as **Protocol**.

3. Select a **Time Synchronization** option.
4. Enter the list of VDV300 telegrams to be recorded. Alternatively, use **New** to enter each element into a separate input field.

Note: Reboot the PCU
To start communication with the defined protocols a reboot must be executed for the PCU (see chapter 3.4).

3.21.3 IBIS (VDV300) Door Client

The PCU is able to act as door client in an IBIS VDV300 network. In this case, an IBIS master controls a number of IBIS VDV300 door clients to get the counting data for recording and the PCU does not need to record the counting data itself. The PCU works in client mode and responds to VDV300 commands sent by the IBIS master. Additionally, system date and time of the PCU can be synchronized with the vehicle time provided by the IBIS master.

Note: To activate the **IBIS-VDV300 Door Client function** of the PCU, the **Client Mode** (see chapter 3.5) must be activated. Otherwise, the PCU records the telegrams received via IBIS (VDV300) and does not respond to commands from the master (see chapter 3.21.2).

Each IBIS-VDV300 door client is uniquely addressed by a door number. The **door number** must be configured for each door client in the IBIS network. It counts from **1 to 16**. Each PCU is responsible for the doors, which are directly connected via SSL bus:

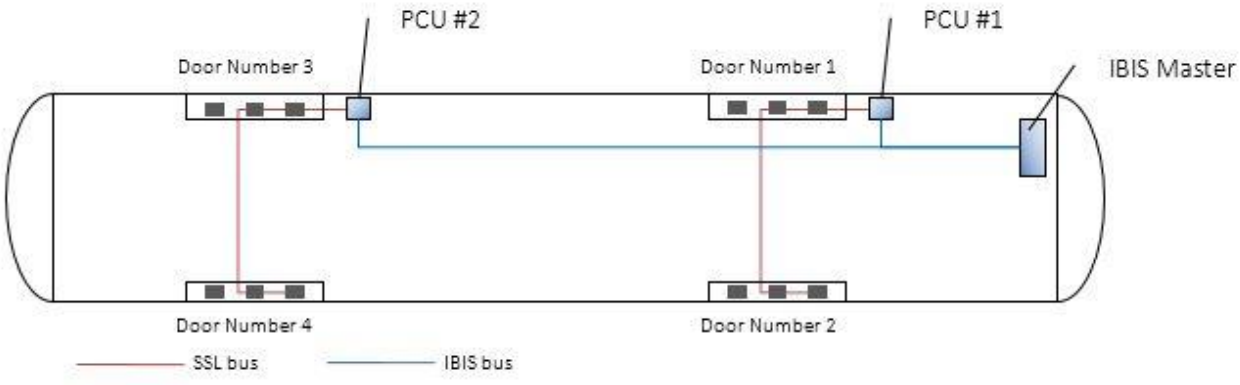


Figure 100: Addressing doors in the IBIS VDV300 bus by door numbers

In the example figure above the PCU #1 is responsible for the doors with the door numbers 1 and 2. The PCU #2 is responsible for the doors with the numbers 3 and 4.

Note: The IBIS VDV300 **door number** is configured by the **Identifier** which can be configured for each door (see chapter 3.7). Enter the door number as identifier, e.g. for door number 3 enter 3 as identifier. Ensure the door numbers are **unique** for the IBIS network and in range from **1 to 16**. The PCU's firmware does not check this.

Note: In order to be able to control a total of **16 doors** via an IBIS-VDV300 master, the PCU enables **door number 16** to be used. **This does not correspond to the IBIS-VDV300 specification. Please only use this capability if it is supported by the IBIS-VDV300 master.**

VDV300 data is received and sent via a serial interface (baud rate 1200 bps, 7 data bit, even parity bit and two stop bits). For the connection of the IBIS bus see chapter 2.4.9.

Configuring an IBIS protocol for door client function

Open the **Configuration > Communication > Comm. Protocols** page to activate the IBIS (VDV300) interface.

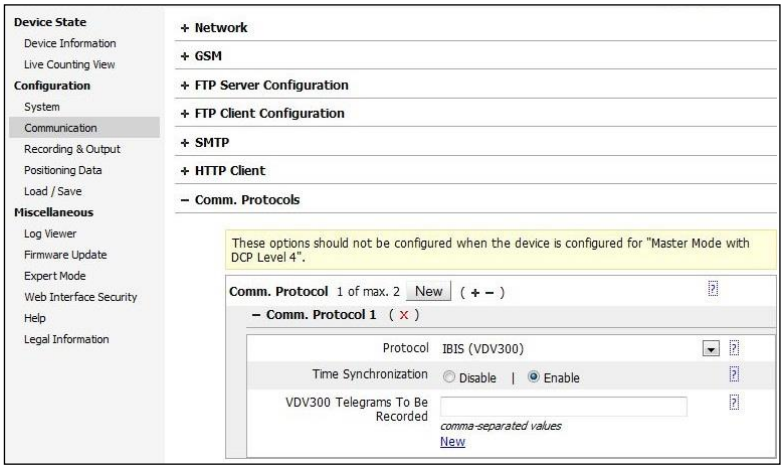


Figure 101: Configuration of the IBIS-VDV300 door client function

1. Press the **New** button next to **Comm. Protocol** to create a protocol profile.
2. Select "IBIS (VDV300)" as **Protocol**.
3. Select a **Time Synchronization** option.
4. Enter the list of telegrams to be used instead of the standard VDV300 telegrams. Leave this field blank if you are using the VDV300 standard implementation. Alternatively, use **New** to enter each element into a separate input field. Possible values are:

Value	Description
DS183a	Uses the counting data response telegram DS183a (bEEEAAA<CR>P) with a larger range of counting values instead of the response telegram DS183 (bEEAA<CR>P).
DS184a	The content of the status response telegram deviates from the standard VDV300 implementation (DS184). The state value 2 (= Counting not finished yet) will be sent even if the door is closed and the "Travel Started" telegram (DS082) was not yet received.

Note: Reboot the PCU
The PCU needs to be rebooted after any configuration change (see chapter 3.4).

3.21.4 DCP Level 1 Protocol

When the master PCU and the client PCUs cannot be connected via Ethernet (because there is no Ethernet network in the vehicle), it is possible to connect them via an RS485 bus instead. The DCP Level 1 protocol defines an alternative network layer for the DCP Level 2 (which implements the DCP Master-Client behavior of the PCUs). This network layer uses a two-wire RS485 bus system for exchanging DCP Level 2 datagrams. To use this function, the PCU must be equipped with the RS485 network interface and the RS485 bus must be connected to the X01 connector (see chapter 2.4.3 for more information).

The devices connected to the RS485 bus via DCP Level 1 have their own DCP Level 1 address, which must be unique in the bus.

Note: Using DCP Level 1, the role of the PCU (**DCP Master** and **DCP Client**) must be configured on the **Configuration > System > General** page as well as on the **Configuration > Communication > Comm. Protocols** page by selecting either the DCP Level 1 Master address, or one of the DCP Level 1 Client addresses.

A DCP Level 1 network can be established with one master and up to 15 clients. When the DCP Level 1 master address is selected, the clients managed by the master have to be configured in the **Configuration > System > Clients** page (see 3.19.2).

The maximum length of the complete RS485 bus must not exceed 500 m. The bus has to be terminated by 120 Ohm termination resistors at each end. Only use twisted pair cables providing shield for the RS485 network. The maximum length between a client and the RS485 backbone can be 2 m. Please note that the cable shield has to be connected only at one end of the RS485 (PCU housing ground). The DCP Level 1 functionality (via RS485) is conform to the standard ISO 8482.

Open the **Configuration > Communication > Comm. Protocols** page to activate the DCP Level 1 interface.

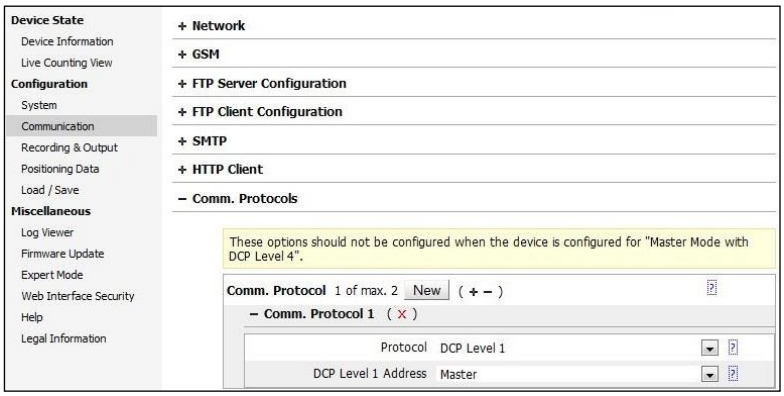


Figure 102: Configuration of the DCP Level 1 protocol

1. Press the **New** button next to **Comm. Protocol** to create a protocol profile.
2. Select "DCP Level 1" as **Protocol**.
3. Select the **DCP Level 1 Address** (either **Master** or one of the client addresses **Client 1…Client 15**).

3.22 Configuration > Recording & Output > Digital Outputs (PCU-220 and PCU-250)

The PCU-220 and the PCU-250 have four digital outputs. These outputs can be configured to signal states of the PCU itself, of the vehicle, and of the passenger counting system. Open the page **Configuration > Recording & Output > Digital Outputs** for configuration:

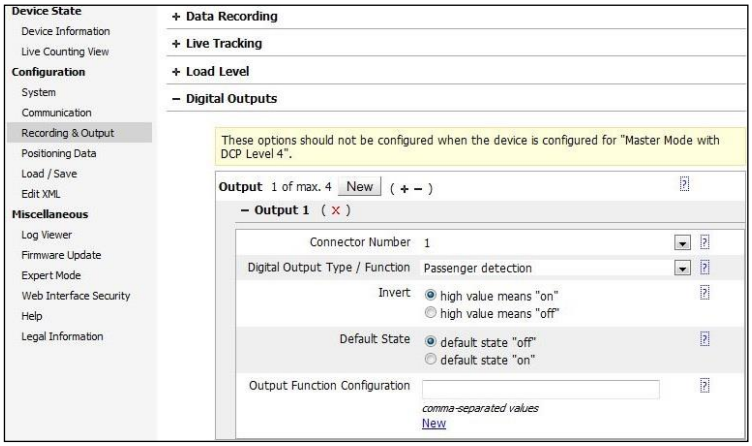
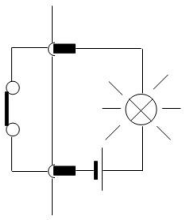
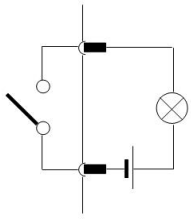


Figure 103: Configuration of the Digital Outputs

1. Press the **New** button to create the settings for a digital output.
2. Select the **Connector Number** (see chapter 2.4.9.2 for the connector names).
3. Select the **Digital Output Type / Function** which describes the meaning of the state the digital output will signal.
4. Select the **Invert** behavior of the digital output depending on the logic of the device consuming the digital output signal:

Invert: High value means "on"	
Logical Signal	Electrical Signal
on	
off	

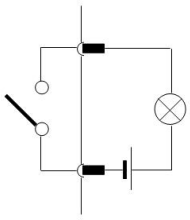
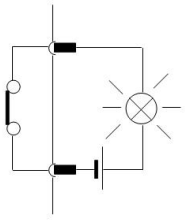
Invert: High value means "off"	
Logical Signal	Electrical Signal
on	
off	

Table 49: Inversion behavior of a digital output

Select the **Default State**. This is the logical state the digital output is set when:

- The system starts after power on or reboot.

- The digital output is configured the first time or the configuration changes.
- An error state of the digital output function is detected (secure state).

Enter the **Output Function Configuration** (see section Passenger Detection for more information). Alternatively, use **New** to enter each element into a separate input field.

Passenger Detection

For passenger counting, the sensors located at the top of a door trigger an event every time an object/passenger of a certain minimum height comes into the area of detection. The PCU registers these events and calculates the incoming and outgoing passengers. The passenger detection function signals the occurrence of such an event during a certain sampling period. A door control can use the passenger detection signal for example to prevent a door to be automatically closed when a passenger inside the vehicle is close to the door.

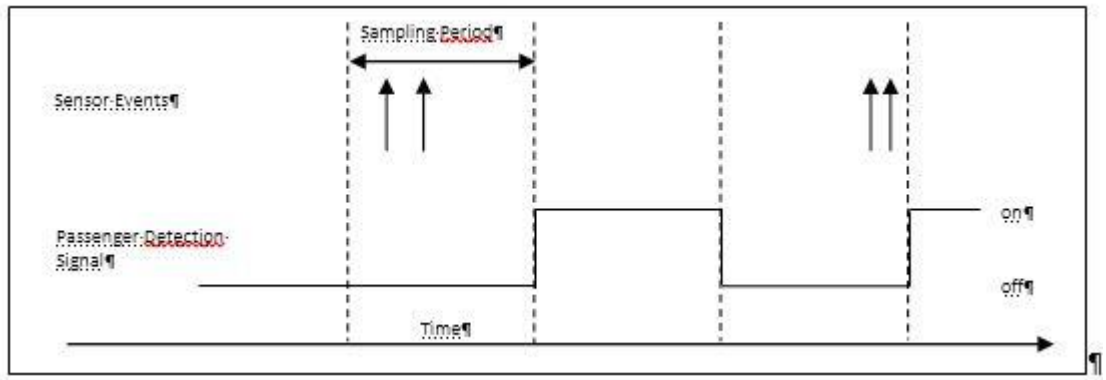


Figure 104: Generation of the passenger detection signal

Use the field **Output Function Configuration** to configure the sampling period and the assigned sensors. The configuration is a comma separated list of numbers.

Example: 250,1,2,3

The first number is the sampling period in ms. This value is mandatory and goes from 10 to 60000.

The following numbers are a list of the SSL positions of the sensors which should be included in the passenger detection function. The values go from 1 to 12.

The example above defines a sampling period of 250 ms and includes the first three sensors.

Note: The configuration of the passenger detection function is independent from the configuration of the passenger counting function. You can use it together with the counting function or as a standalone function.

Hint: To get **one passenger detection signal per door**, create one digital output configuration set for each door by pressing the **New** button. Assign a unique digital output connector to each door and configure the SSL positions of the door's sensors for the corresponding configuration set.

Error Signal

When the option **Error signal** is selected at **Digital Output Type / Function**, the digital output is configured to signal any error state of the passenger counting system.

In a typical application case, the digital output of a master PCU is connected with a digital input of an onboard unit. Therefore, the onboard unit is able to detect the state of the whole vehicle including the passenger counting system. The master PCU signals its own error state as well as the error state of the connected client PCU's.

If the PCU is configured to be a client, only the own error state is signaled.

When the error state vanishes, the error state signal will be released automatically.

Between the occurrence of an error state change and the change of the error signal at the digital output a maximum delay of 20s can occur.

Note: The error signal function does not require an entry in the **Output Function Configuration** field. This field can be left empty.

Counting Impulses - Boarders and Counting Impulses - Alighters

When one of the options **Counting Impulses - Boarders** or **Counting Impulses - Alighters** is selected at **Digital Output Type / Function**, the digital output creates an impulse for every person (boarding or alighting) counted by the PCU. Counting is carried out for all doors which are directly connected to the PCU via SSL bus. The impulses are generated as soon as the PCU detects a boarder or alighter when at least one door is opened. Even if the door is closed the impulse generation continues until all boarders or alighters are signaled.

The following schema shows the pulse timing:

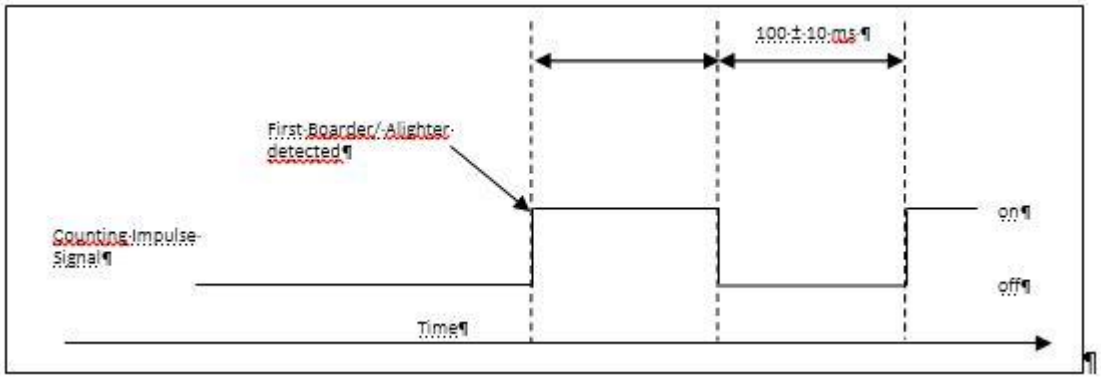


Figure 105: Timing of the counting pulse signal

There is one impulse (signal level "on") per counted boarder or aligther. This behavior can be inverted (parameter **Invert**) so that the default level is "on" and the impulse level is "off".

Note: To use the counting impulses, both digital outputs **Counting Impulses - Boarders** and **Counting Impulses - Alighters** must be configured.

Only two digital output ports can be configured with this function at the same time.

4 Maintenance

4.1 Clock Synchronization

The PCU is not equipped with a real time clock. Its system time is reset to January 1st 1970 00:00:00 UTC at every time the system is powered up. If an SNTP server is configured, the PCU will synchronize its clock automatically every 60 minutes. If the PCU gets its IP address of the SNTP server dynamically by DHCP, the PCU will synchronize its clock automatically every time it gets a new DHCP lease or the DHCP lease is extended. If the SNTP server cannot be reached, the PCU will try to reach the SNTP server automatically every 20 seconds.

The clock cannot be set via the web interface, except in expert mode, see chapter 5.18.

Note: Time synchronization can only be carried out with **one** source in the counting system. SNTP (via Ethernet, Wi-Fi, or GSM), GPS, or IBIS can be configured as a source. If none of these sources is configured, the PCU attempts to receive the system time via DCP.

In a master client environment, the source can be connected directly to the master or to a client. Always prefer time synchronization with a source which is directly connected to the master PCU. Only use a client PCU for this functionality, if there is no other possibility.

4.2 Loading / Saving the Configuration from or to a File

With the page **Configuration > Load / Save** the configuration of the PCU can be stored in an XML file. This file can be used later to restore the configuration to the device (e.g. when the device must be replaced).

This menu can also be used to upload an XML file to the PCU in order to configure the PCU.

4.2.1 Saving the Device Configuration to a File

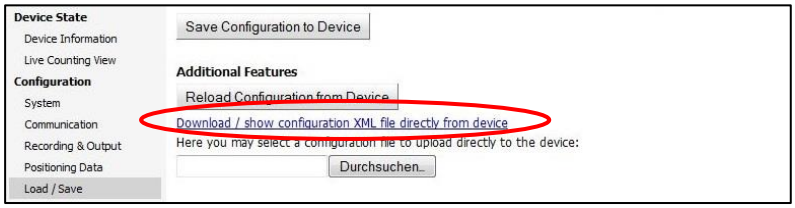


Figure 106: Downloading a configuration as XML file

Download of the configuration file (saving):

1. Open the page **Configuration > Load / Save**
2. Click on the link **Download/show configuration XML file directly from device**.
   A new browser window appears which displays the content of the XML file.

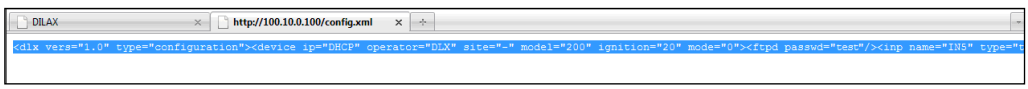


Figure 107: The configuration is shown in a new browser window

Alternatively you can click on **Download/show configuration XML file directly from device** with the right mouse key and select **Save target at** for saving this file.

3. Save the displayed site as text file.

Note: We recommend to end the file name with "config", e.g. "PCU-200_Test_config.xml". This makes it easier to identify the file later.

Warning: The configuration will be directly loaded from device. If you are currently editing the configuration in the web interface please first save the configuration (button **Save Configuration to Device**) before downloading it.

4.2.2 Loading the Device Configuration from a File

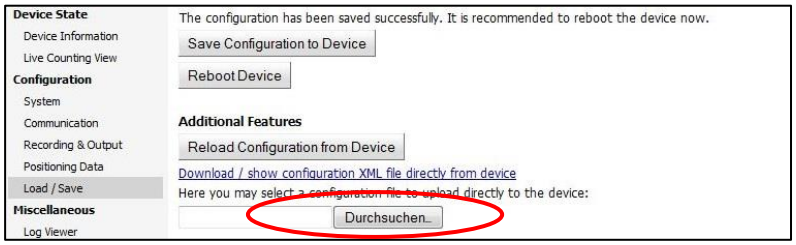


Figure 108: Loading a configuration from an XML file

To load (upload) a configuration file:

1. Open the page **Configuration > Load / Save**
2. Click the **Browse** button.
3. A dialog appears.
4. Select a configuration file and click the open button.
5. A success message will appear when the configuration is uploaded and validated successfully. Otherwise an error message will appear.

4.2.3 Validate hardware configuration

The firmware allows to validate a configuration without adopting it to the hardware.

Perform the following steps:

1. Open page Configuration > Load/Save
2. Activate „Extended Configuration Options“
3. Select „Upload and only validate a configuration file“
4. Press button **Durchsuchen**
5. A dialog window is opened
6. Select the desired configuration file and press button open. The configuration file is not loaded to the hardware device.
7. After successful validation, a positive message is given. If not, an error message is displayed.

4.2.4 Extended Configuration Options for Loading the Device Configuration from a File

There may be specific situations where the configuration of the PCU depends on the place of installation. For these installations, the configuration plug SST-100 is preferred, which stores the appropriate installation (see chapter 4.3). The SST-100 always remains at the place of installation. If the PCU must be replaced, the new PCU will be configured with the SST-100 and will afterwards have the same characteristics as the old PCU.

If the SST-100 cannot be used, e.g. by mechanical reasons, a set of configuration files (consist configuration package) may be stored on the PCU. This set is a tar archive which contains one configuration file for each possible place of installation. After system start, the PCU detects by itself at which place it is installed, selects the correct configuration file from the set and configures itself.

Attention: The mechanism for detecting the place of installation depends on the vehicle and must be customized before it can be used.

Use the extended configuration options for:

1. Validating single configuration files,
2. Uploading and saving a consist configuration package to the PCU,
3. Downloading and locally saving a consist configuration package from the PCU.

Validating a single configuration file

Before a consist configuration package is uploaded and saved to the PCU, the single configuration files of the package can be validated.

Figure 110: Validating a single configuration file

Proceed as follows to validate a single configuration file by the PCU:

1. Activate the **Extended Configuration Options** check box.
2. Select the **Upload and only validate a configuration file** option.
3. Click the Browse button.

   A dialog appears.
4. Select a configuration file and click the open button.

   The file will be uploaded to the PCU but not saved, checked by the PCU, and deleted. Afterwards you will receive information about the result.

Uploading and saving a consist configuration package to the PCU

A consist configuration package is a tar archive which contains several configuration files. It will be uploaded to the PCU. At system start the PCU automatically configures itself with the correct configuration file from the package; this depends on the place of installation.

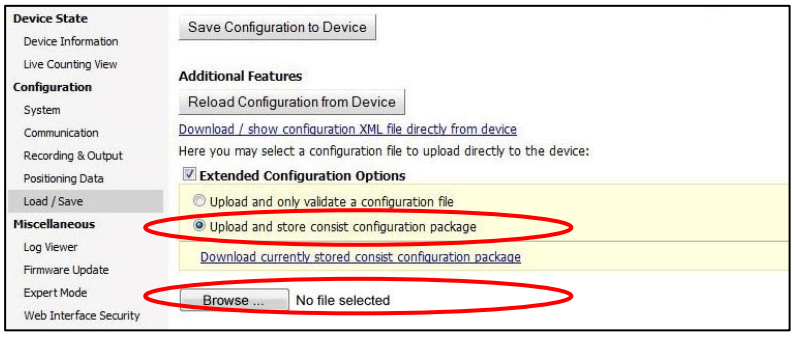


Figure 111: Uploading and saving a consist configuration package

Proceed as follows to upload and save a consist configuration package to the PCU:

1. Activate the Extended Configuration Options check box.
2. Select the Upload and store consist configuration package option.
3. Click the Browse button.

   A dialog appears.
4. Select the tar archive and click the open button.

Note: The tar archive must contain at least one configuration file named "config.xml".

A success message will appear when all configuration files of the package have been uploaded, validated and saved successfully. Otherwise an error message will appear.

It is recommended to reboot the device when a configuration has been saved successfully. Therefore click the **Reboot Device** button.

Downloading and locally saving a consist configuration package from the PCU

A consist configuration package is a tar archive which contains several configuration files. It can be downloaded from the PCU and saved locally.

Figure 112: Downloading a consist configuration package

Proceed as follows to download a consist configuration package from the PCU and save it locally:

1. Activate the Extended Configuration Options check box.
2. Click on the hyperlink Download currently stored consist configuration package and save or open the tar archive.
3. Alternatively you can click on the hyperlink with the right mouse key and select Save target at for saving the file.

4.3 Usage of the Configuration Plug

To use the configuration plug, the PCU must be equipped with the configuration plug connector X12 (see chapter 2.5.1). A configuration plug is a non-volatile storage.

The configuration plug can be used in two different modes. First, the configuration plug is permanently connected to the PCU. Second, the configuration plug is temporarily plugged on the PCU to automatically distribute a master configuration to a lot of devices.

Do not confuse master configuration with configuration of a master PCU. A master configuration is stored at a configuration plug used to configure PCUs. The configuration of a master PCU is stored in the PCU which is configured in master mode.

4.3.1 Permanent Mode

This mode is used to simplify the replacement of a PCU in a maintenance process. With the first installation of the PCU, the configuration for the certain place of installation is created and stored on the configuration plug. Once the PCU has to be replaced, its configuration plug must be plugged on to the new device. When the new device is started, it will automatically be configured with the configuration stored on the configuration plug. There is a two-step process for the **permanent** mode:

1. Creating a configuration and saving it on the configuration plug

1. Ensure the configuration plug is always plugged on to the PCU.
2. Start the PCU.
3. On the page **Configuration > System > General** select **Permanent** as **Configuration Plug Mode** (see chapter 3.5).
4. Edit the configuration of the PCU.
5. Save the configuration as described in chapter 3.4.

Repeatedly saving the configuration overrides the configuration on the configuration plug and the PCU.

Notes: The configuration is stored on both the configuration plug and the non-volatile memory of the PCU. If the configuration plug is not connected, the configuration cannot be stored on the configuration plug, a warning message appears and the configuration will be stored on the PCU.

If the configuration is not valid, an error message will be displayed and the configuration will not be stored on the configuration plug. The old configuration remains on the PCU and the plug.

If the configuration plug is unplugged after saving, the configuration remains on the PCU. If the configuration plug is plugged again, the PCU starts with the configuration from the configuration plug after next reboot (forced via web interface or normal boot up/shutdown procedure). The settings of the PCU will be overwritten.

2. Configuring a PCU using the configuration plug (in case of replacement)

1. Attach the configuration plug with a valid configuration in order to transfer this configuration to the PCU.
2. Start the PCU. This loads the configuration from configuration plug.

Note: If you try to configure a PCU with a configuration plug containing no or an invalid configuration, the configuration stored in the non-volatile memory of the PCU will be used to configure the device. A log message is shown in the system log (see chapter 5.1).

4.3.2 Auto Mode

This mode is used to simplify the distribution of a master configuration to a lot of PCUs, without using the Ethernet interface and the web interface. Once a master configuration is created and stored on the configuration plug, it can be distributed to other PCUs by temporarily plugging the configuration plug to each of the PCUs. There is a two-step process for the **auto** mode:

1. Creating a master configuration and saving it on a master configuration plug

1. Select a PCU, where the master configuration can be created. Preferably, it should be a device which should also be configured with the master configuration.
2. Ensure the configuration plug is plugged on to the PCU.
3. Start the PCU.
4. On the page **Configuration > System > General** select **Auto** as **Configuration Plug Mode** (see chapter 3.5).
5. Edit the master configuration of the PCUs.
6. Save the configuration as described in chapter 3.4.

Repeatedly saving the configuration overrides the configuration on the configuration plug and the PCU.

Notes: The configuration is stored on both the configuration plug and the non-volatile memory of the PCU. If the configuration of the PCU is changed via web interface, the configuration plug must be connected, otherwise an error message appears and the configuration will not be stored – neither in the PCU nor at the configuration plug. The old configuration remains on the PCU.

If the configuration is not valid, an error message will be displayed and the configuration will not be stored – neither in the PCU nor at the configuration plug. The old configuration remains on the PCU and the plug.

If the configuration plug is unplugged after saving, the configuration remains on the PCU. If the configuration plug is plugged again, the PCU starts with the configuration from the configuration plug.

2. Distributing the master configuration to the PCUs

1. Put the new PCUs to their original place of installation and connect all electrical wires.
2. Power on the PCUs.
3. Attach the configuration plug with the master configuration at the first PCU and wait until the PCU makes a reset (the read error LED goes off, than on for about 5s and off for at least 5s).
4. Unplug the configuration plug and repeat the last step for the other PCUs to configure.

Note: If you try to configure a PCU with a configuration plug containing no or an invalid configuration, the configuration stored in the non-volatile memory of the PCU will be used to configure the device. A log message is shown in the system log (see chapter 5.1).

4.3.3 Requesting the State of the Configuration Plug

The configuration plug state is shown on the **Device State > Device Information > Hardware Present** page.

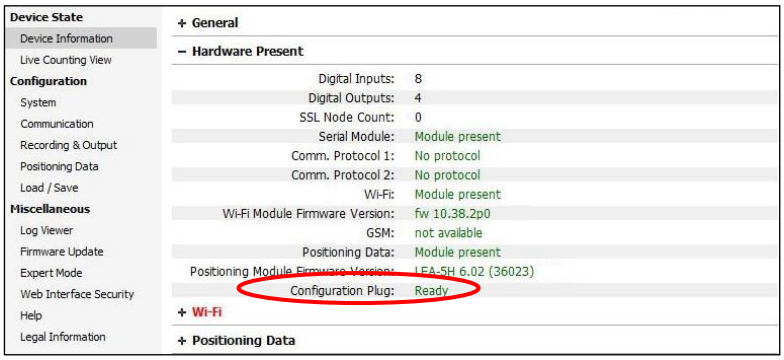


Figure 113: State of the configuration plug

If no configuration can be read from the configuration plug or the configuration stored on the plug is invalid, an error state is shown.

If the configuration cannot be stored on the configuration plug, an error state is shown, too.

In **Permanent mode**, missing the configuration plug is shown as an error.

In **Auto mode**, missing configuration plug is a normal state and no error. The configuration plug is unplugged.

4.4 Firmware Update

Before starting an update for a higher number of vehicles, update only one vehicle to validate update and functions. This update should be performed inside the vehicle. After successful validation, update all the rest of the vehicle via remote connection.

There are two possibilities to update the firmware:

- Update via web interface
- Automatic update via FTP

Warning: Ensure the PCU is not switched off during firmware update.
The firmware update will not be correctly completed when the PCU is switched off during a firmware update.

Notes:

The configuration will not be changed during a firmware update.
Please refer to the provided release notes for implications on the configuration after a firmware update (upgrade). We recommend to verify the existing configuration before starting a firmware update (see chapter 5.19). Firmware downgrades are not recommended without contacting the DILAX support.

Delete the customer profile before downgrading
Before downgrading the firmware, delete the **Customer Profile** on the page **Configuration: General**. When the downgrade was successful you can add a customer profile, if necessary. In case of a firmware upgrade it is not necessary to delete the customer profile.

4.4.1 Firmware Update via Web Interface

If necessary, DILAX will provide a firmware image file to update the firmware of the PCU. Please read the provided release notes before starting an update. Do not use a GSM dial-in connection for executing the firmware update (see 4.5).

The file name of the firmware image has the following format:

NAME_VERSION.img

Example: PCU-200_1.0.0.img

Note: During a firmware update the system log will be deleted. To track operations retrospectively, you should download and save the system log before a firmware update.

1. Open the menu **Miscellaneous > Firmware Update** to upload a new firmware image file to the PCU.

Figure 114: Starting a firmware update

2. Click the **Browse** button. Select the firmware image file on your local computer and confirm it.

   You will be asked to confirm the update process.

3. Confirm the update process.

First the integrity of the firmware image will be verified and the compatibility will be checked. Then the update is performed. During the update status information are displayed and requests appear which need to be confirmed. Please always pay attention to the status information.

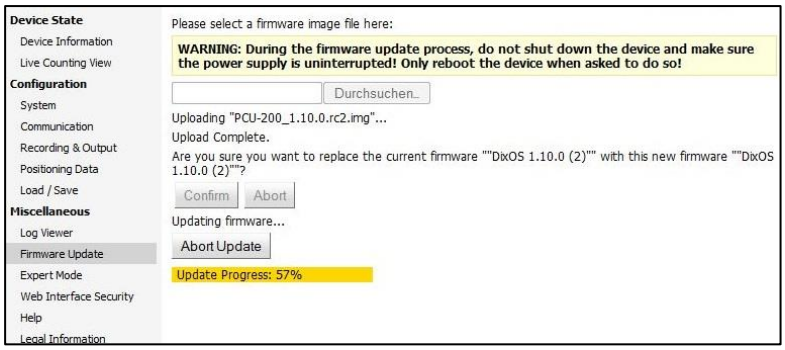


Figure 115: Status information and requests during a firmware update

The update process can be aborted at any time by clicking the corresponding **Abort** button.

When there is a power-failure during the update, the process will be aborted automatically and the device will fall back to the firmware version previously used.

After an update the device will be rebooted automatically. Check the device information (page **Device State > Device Information**) to verify the update of the new firmware version.

P1 1.10.6.1.2

4.4.2 Automatic Firmware Update via FTP

If there is no access to the PCU via web interface, you can (remote) update the firmware by the FTP client function of the PCU.

Prepare the PCU Configuration

To enable this update feature, configure the FTP client function of the PCU as described in chapter 3.12. Please note your FTP settings, you will require them later for script file creation.

At the menu **Configuration > System > General** you must configure the fields **Operator Name** and **Site Or Vehicle Name**.

Prepare the FTP Host

At the FTP host, configured by the **FTP Hostname** in the FTP client configuration (page **Configuration > Communication > FTP Client Configuration**), add a new directory named "scripting" at the data directory configured in **Path**.

Example:
FTP Path is /home/XXX/
Create the directory: /home/XXX/scripting

1. Copy the firmware image file to the "scripting" directory.
2. Prepare the update script file

   Together with the firmware image, DILAX publishes script file templates for the firmware update.

   script_fw_update_gsmtemplate_operator_site.sh
   Used for the remote update via GSM/GPRS or Ethernet. (see Figure 127)

```
################################################################################
# description   : Example script for PCU-200
# autor         : ---
# date          : 20.10.2010
################################################################################
# script version: 20102010
################################################################################

# Get firmware and script

ftpget <hostname> <ftpusername> <ftppassword> <ftppath>/scripting/PCU-200_1.0.0.img /PCU-200_1.0.0.img

# Update master firmware

firmware install /PCU-200_1.0.0.img

firmware reboot
```

Figure 116: Script file template for firmware update

3. Copy the appropriate template to a local directory and open it with a text editor.
4. Replace <hostname> with the IP address or the host name of the host
   (page Configuration > Communication > FTP Client Configuration, parameter FTP Host).
5. Replace <ftpusername> with the value of the FTP user name
   (page Configuration > Communication > FTP Client Configuration, parameter Username).

6. Replace <ftppassword> with the value of the FTP password
   (page Configuration > Communication > FTP Client Configuration, parameter Password).

7. Replace <ftppath> with the value of the FTP path
   (page Configuration > Communication > FTP Client Configuration, parameter Path).

Example:
FTP Host = test.com.ftp
Username = usertest
Password = testpassword
Path = /home/XXX

Example replacement looks like:
ftpget test.com.ftp usertest testpassword /home/XXX/scripting/PCU-200_1.0.0.img /data/ftp/system/PCU-200_1.0.0.img

8. Save the script file with the name: script_<operator>_<site>.sh

9. Replace:
   <operator> with the Operator Name configured on page Configuration > System > General
   <site> with the **Site Or Vehicle Name** configured on page **Configuration > System > General**

Example:
Operator Name = TEST
Site Or Vehicle Name = B-TE-4711
Rename the example file to: script_TEST_B-TE-4711.sh

10. Copy the script file to the directory "scripting".

4.5 Remote Access via GSM Dial-In

If your PCU contains a GSM module you can dial in to the PCU to get access to the web interface and the build-in FTP server. This feature is intended to be used during trouble shooting and maintenance.

Note: A dial-in connection via GSM has a very low baud rate of 9600 bits per second. These leads to long download and upload times up to several minutes. For this reason, do not execute a firmware update via web interface by using a GSM dial-in connection.

If the PCU is equipped with a 3G module instead of a GSM module, dial-in is not possible.

Requirements

To use this feature, the PCU must be equipped with a SIM-card supporting a dial-in data service. Please contact your GSM provider whether this service is enabled for the SIM-card or not.

A phone number to call the PCU.
This can be an extra number, separated from the number used for voice calls.

A modem at your workplace. This can be an analogue modem, a GSM modem, or a mobile phone with modem function.

A phone line for far calls in case of an analogue modem, or a SIM-card with dial-out connections enabled (for a GSM modem).

The configuration data of the PCU to connect to: PPP server user name, PPP server password and PPP server IP address (see chapter 3.11).

Note: In the GSM configuration, the **Dial-on-demand Routing** must be set to **Dial on demand**, otherwise it is not possible to establish a dial-in connection to the PCU.

Preparation

Connect the modem or the mobile phone with your local computer (via USB, RS232, or Bluetooth depending of the modem used).

Install the modem's driver if not already done (see the modem documentation for details).

Create a dial-out connection on your local computer (sometimes called Remote Access Service connection, RAS connection). See the documentation of the operating system for details. Insert the phone number of the PCU as number to dial as well as the PPP server user name and the PPP server password for authentication.

Start the dial-out connection. See the documentation of the operating system for details of how to establish a dial-out connection.

Wait until the dial-out connection is established (during dial-out, the operating system shows state information).

Using the Web Interface

To use the web interface for remote configuration or trouble shooting:

1. Open the browser and insert the address line with the PPP server IP address:

Example: http://199.166.0.1/?long_timeouts=1

Note: The address extension **?long_timeouts=1** allows the usage of the web interface for the very low speed GSM connection. Without using this extension time out errors messages may occur.

The load time of the web interface can be up to five minutes.

2. Use the web interface.

Note: A running GSM dial-out connection will be lost when the PCU is rebooted via web interface.

Note: Do not use web interface functions intended to test the GSM/GPRS connection. A running GSM dial-out connection will be lost when the functions **Start FTP Transmission Now** (see chapter 3.13) or **Start SMTP Transmission Now** (see chapter 3.14) are executed.

Using the build-in FTP server

You can use the build-in FTP server of the PCU to access counting data, upload scripts etc.

Use a common FTP client program and configure the FTP connection using the PPP server IP address as FTP server address. Configure the FTP server log in as described in chapter 3.12.

5 Troubleshooting

5.1 Logging, Error Handling and Watchdog

Log messages are usually stored in the persistent flash memory. If the current log file grows up to a fixed file size limit it will be closed and a new log file will be created. This way, several log files will be created. When the number of log files exceeds a fixed limit, the oldest log file will be deleted.

If an event triggers a log message with the priority "fatal" the PCU will be rebooted immediately. This will ensure that the PCU continues counting with a less of down time. Already recorded counting data and the configuration will not be lost.

The PCU is equipped with a hardware watchdog. If the software is not responding for approximately 30 seconds the watchdog will raise a log message with the priority "fatal" and the PCU will reboot immediately.

To prevent infinite loops of reboots due to an invalid configuration the PCU has a build in reboot loop detection. If the PCU detects a loop (up to 6 automatic reboots during system start within 12 minutes are required for detection), it goes into the **first Fail-Safe Mode** by loading a fail-safe configuration. The fail-safe configuration is generated from the actual configuration by copying the network settings in a factory configuration. So, the PCU still can be accessed via Ethernet network and the configuration can be corrected.

Note: In the **first Fail-Safe Mode**, the current configuration remains available via web interface, while the PCU has loaded a fail-safe configuration in the background. This should help you to easily correct the configuration. Have a look into the system log view to determine the reason for the reboot loop and correct the configuration. As soon as you save the configuration by means of the web interface, the fail save configuration will be overridden by the saved configuration. You have to reboot the PCU to deactivate the Fail-Safe Mode.

If it is not possible to generate the fail save configuration in the first Fail-Safe Mode, the PCU goes into the **second Fail-Safe Mode**. In this mode, the PCU uses the factory settings, where the Ethernet network interface is configured with the fix IP **192.168.23.200** and the subnet mask **255.255.255.0**.

Log messages can be displayed in the web interface. Open the web interface of the PCU and select the page **Miscellaneous > Log Viewer**.

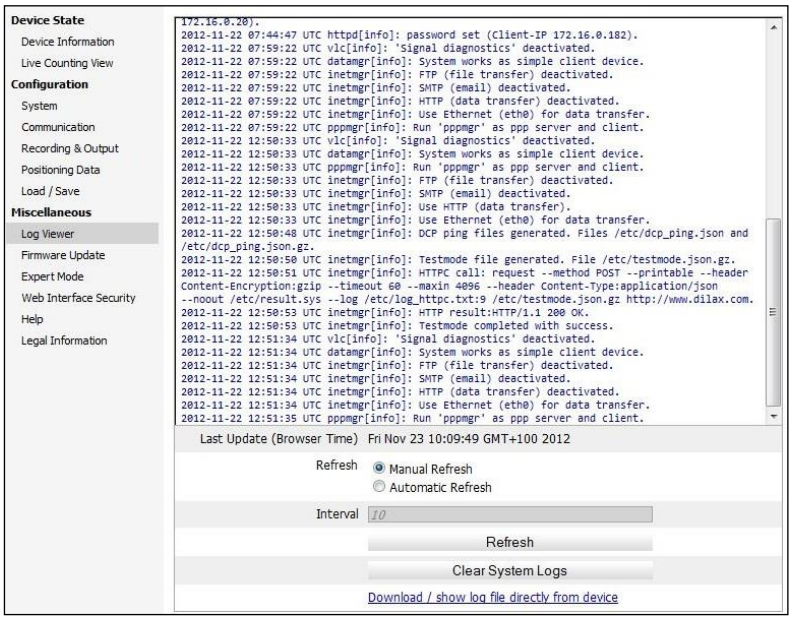


Figure 117: Log viewer

In order to save the displayed log file click on **Download / show log file directly from device** with the right mouse key and choose "Save target at".

View the Current Log Entries

The web interface does not refresh the log viewer display automatically. To get the currently logged data press the **Refresh** button.

For an automatic, periodically refreshing activate **Automatic Refresh** and enter the time interval in the input field **Interval**.

Clear the Log

To restart the log message recording of the PCU press the button **Clear System Logs**. This deletes all log files and starts a new one.

The log messages contain the following elements (example):

2010-10-08 10:51:06 UTC httpd[debug]: GET /banner.png (Client-IP 172.16.0.166).

Element	Example	Description
Timestamp	2010-10-08 10:51:06 UTC	Date and time when the event occurred. If no valid system time is available, the system time starts at January 1 1970 00:00:00 UTC.

Module	httpd	Originating module: e.g. kernel, application, network, FTP, IPTCom, TDC or HTTPD.
Priority	[debug]:	Event priority: fatal error warning info debug
Message	GET /banner.png (Client-IP 172.16.0.166).	Log message. In the case of an error the message also contains the source code filename and a source code line number to support the customer service.

Table 50: Log entry elements

Error messages that are associated with an error code are not only saved in the system log but also indicated on the red error LED of the device. Please refer to section 5.16 for a list of error codes.

5.2 Creating an error report

In case of problems you can create a standardized error report at **Expert Mode > Report A Problem** in order to get it analyzed by the DILAX Customer Service.

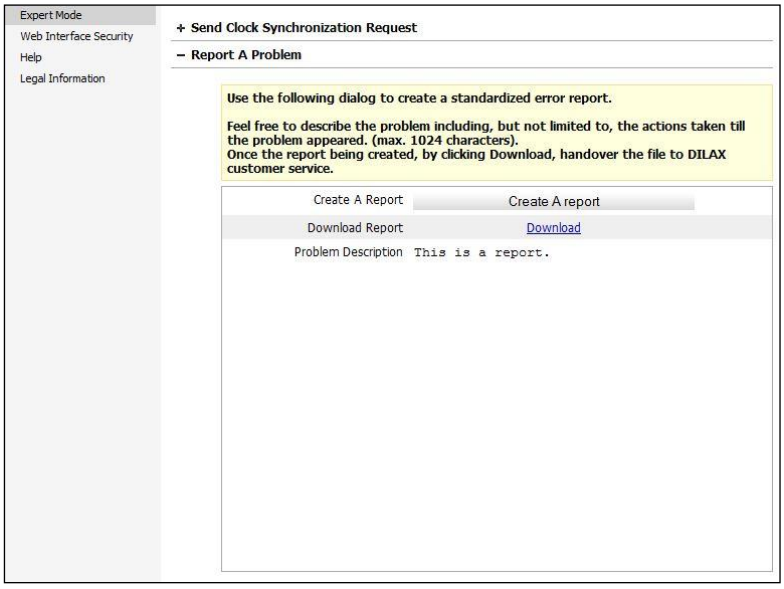


Figure 118: Creating an error report

1. Enter a description of the problem into the **Problem Description** input field. In addition, mention the steps which have been executed before the problem occurred, so that the DILAX Customer Service can reproduce the occurrence.

Note: A maximum of 1024 characters are available for the description.

2. Click the **Create a report** button to generate the error report.

   As soon as the error report is available in file format, click **Download**. You can open the file or save it on your computer.

3. Send the file to the DILAX Customer Service or directly to your contact person at DILAX.

5.3 Unlock Web Interface When Password is Lost

When the password for accessing the web interface is lost you can request a “daily password” to unlock the web interface. Call the DILAX Customer Service to get the daily password.

You will be asked for the current system date (local date including the time zone setting). This must be the system date of the PCU where you want to unlock the web interface. If you are not sure what the system date is, follow these steps:

1. Open the web interface. The browser shows the authentication dialog box.

Figure 119: Authorization dialog box

2. Press the **Cancel** button. An error message appears which contains the current system date. The format is Year/Month/Day.

3. Remember the system date.

After requesting the daily password from the DILAX Customer Service, login with the user name "dilax" and the received password.

First configure a new password for accessing the web interface (see chapter 3.3).

5.4 Testing Sensor Setup

The sensor setup can be tested using the **Device State > Live Counting View** (displays counting data) as well as the **Device State > Device Information** (additionally displays device status information including door contact state and error codes).

5.4.1 Device State > Live Counting View

Select the page **Device State > Live Counting View** to display counting data and to verify the sensor setup.

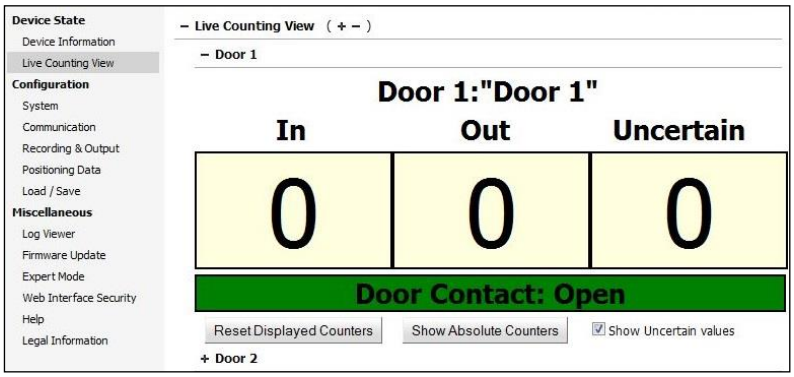


Figure 120: Live Counting View

Counting data is displayed per door. Expand the section of the appropriate door. The page is refreshed automatically. It shows the following information for the selected door:

Information	Description
In	Number of people entered.
Out	Number of people left.
Uncertain	Number of unclassifiable artifacts (only visible when **Show Uncertain values** is activated).
Bar below **In**, **Out** and **Uncertain**	If a door contact is configured for the selected door its status is displayed. When there is an error affecting a sensor or door contact it will not only be logged in the system log and shown on the red error LED (see section 2.4.11) but it will also be displayed on this bar on the web interface. The bar changes its color to red.

Table 51: Live Counting View – Displayed information for a door

When you open this page absolute values are shown for **In**, **Out** and **Uncertain**. Absolute values are the total values since the last system boot.

But there are situations where you only need to see intermediate values, e.g. the values for the stop a vehicle arrives next or the values of people entering/leaving within the next 5 minutes. In this case, click the button **Reset Displayed Counters** and the three values will be set to 0 (zero). This action does not reset the absolute values, it only changes the currently displayed values. Click on the button **Show Absolute Counters** to return to the absolute values of the selected door.

5.4.2 Device State > Device Information

Select the page **Device State > Device Information** to display counting data and, in addition, the device status information. This information includes the door contact state and any error codes for each door.

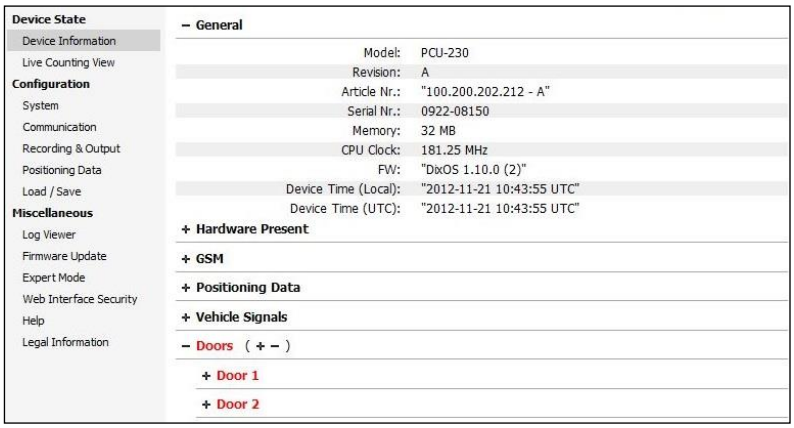


Figure 121: Device information (example)

The page is refreshed automatically. It shows the following information for each door:

Information	Description
In	Number of people entered through this door since the last system boot.
Out	Number of people left through this door since the last system boot.
Uncertain	Number of unclassifiable artifacts at this door since the last system boot.
Door contact state	If a door contact is configured for the door its status is displayed. When there is an error affecting a sensor or door contact it will not only be logged in the system log and shown on the red error LED (see section 2.4.11) but it will also be displayed on this bar on the web interface. The bar changes its color to red.
Error Code	Number of error codes occurred at the door. Error code 0 indicates an error free state.

<table>
<tr><th>Information</th><th>Description</th></tr>
<tr><td>Error supplement</td><td>Additional, detailed information to the error code:
<table>
<tr><th>Error code</th><th>Description</th></tr>
<tr><td>0</td><td>no supplementary information</td></tr>
<tr><td>1</td><td>The PCU device is not responding.</td></tr>
<tr><td>2</td><td>Not enough nodes connected to the SSL bus.
The error supplement code is the SSL position (counting starts at 1) of the first missing sensor of the door.</td></tr>
<tr><td>3</td><td>Flickering sensor.
The error supplement code is the SSL position (counting starts at 1) of the flickering sensor.</td></tr>
<tr><td>4</td><td>SSL bus is not operational.</td></tr>
<tr><td>5</td><td>Sensor is not operational.
The error supplement code is the SSL position (counting starts at 1) of the sensor that reports an invalid bit structure.</td></tr>
<tr><td>6</td><td>Configuration is erroneous.</td></tr>
<tr><td>7</td><td>Door signal unavailable.</td></tr>
<tr><td>8</td><td>Blocked sensor.
The error supplement code is the SSL position (counting starts at 1) of the blocked sensor.</td></tr>
<tr><td>10</td><td>Sensor optic has not detected anything for a long time.</td></tr>
<tr><td>11</td><td>Door contact has not changed its state for a long time.</td></tr>
<tr><td>12</td><td>Sensor has not counted any valid event for a long time.</td></tr>
<tr><td>13</td><td>Counter (counting input) has not counted any valid event for a long time.</td></tr>
<tr><td>20</td><td>Door is erroneously reported as open.</td></tr>
</table></td></tr>
<tr><td>Details</td><td>Numbers of people entered, left and unclassifiable are displayed for every sensor of the door (since the last system boot).</td></tr>
</table>

Table 52: Live Device Status – Displayed information for a door

5.5 Diagnostic Messages

If activated, the master PCU tests the plausibility of its signals and the functionality of sensor and door signals of both itself and the assigned clients.

Example:

The door signal indicates an open door, while the driving signal indicates that the vehicle is driving. This indication is not plausible because the doors should be closed when the vehicle is driving. If this state remains for a certain time, the PCU generates a diagnostic message and records it into the dlx3 record file and into the system log. As a result of this message you should do the following:

The counting data of the door must be excluded from analysis by the background analysis system.

The system does not work as expected. Check the electrical signals (for example the door signal never changes) and the configuration of the PCU (for example the door signal or the driving signal must be inverted).

Activation:

The generation of diagnostic messages can be individually activated for:

Each door in the configuration **of the master PCU and the client PCUs** (see chapter 3.7)

Vehicle signals of the master PCU (see chapter 3.9)

Note: Although only the master PCU generates diagnostic messages, the **diagnostics of the doors** are activated/deactivated in the configuration of the client PCUs where the door is configured. The client PCUs send a signal to the master PCU whether the diagnostics of a door are activated or not. The master PCU processes the diagnostics according to this indication.

The diagnostics of the doors assigned to the master PCU itself are activated/deactivated in the configuration of the master PCU.

Note: When the vehicle is out of operation for a long time, the period of inactivity leads to a generation of diagnostic messages. For example: If the vehicle stays for a long time (> 48h) in a depot, but the power remains on, and no doors are opened, a diagnostic message would be created, because the long term inactivity suggests a failure of the door contact signals. To prevent this, the **Vehicle in operation signal** is used. When the vehicle in operation signal indicates the out of operation state of the vehicle, the monitoring of the doors activity is suppressed until the vehicle goes in operation.

If the Vehicle in operation signal is not configured as **Vehicle signal** (see chapter 3.9) it is calculated by the PCU: After power on it goes to on. The PCU looks whether the vehicle stays at a station for more than 20 minutes and sets the Vehicle in operation signal off until the vehicle starts driving.

Recording:

Diagnostic messages are recorded in:

the system log

the error report e-mails

the dlx3 data recording files

of the master PCU.

Messages:
The following Table 58 describes the diagnostic messages:

Column **DLX3 Identification** contains the identification of the message in the dlx3 data block “DIAG”.

Columns Log Level and Log Message contain the priority and the message in the system log and the error report e-mail. Additionally, column Log-Message describes the determination of the diagnostic message.

Possible measures are described in the column Measure.

DLX3 Identification ModuleID. SubModuleID. MessageID (Category)	Log Level	Log Message and Description	Activated with configuration of:	Measure
20.0.8 (Warning)	Warning	“Sensor <sensor_of_the_door> of door '<door_name>' is blocked. Blocked sensor. The error supplement code is the SSL position (counting starts at 1) of the blocked sensor.	Doors (client and master PCU)	Check if sensor is blocked by s.th. or dirt (e.g. taped with paper). In this case you can disable the diagnostics for this door to prevent unnecessary messages.
20.0.10 (Warning)	Warning	“Optic A of sensor <sensor_of_the_door> from door '<door_name>' at site '<site_name>' has not changed its state since <time_span>.” Checks the signals sent from the sensor for a long time period of vehicle operation (> 48h). The state is determined even if the vehicle occasionally is switched off.	Doors (client and master PCU)	Check the concerned sensor (replace it, if necessary). Check whether the door is out of order and no counting events can be created. In this case you can disable the diagnostics for this door to prevent unnecessary messages.
20.0.11 (Warning)	Warning	“The door signal <signal_number> from door ‘<door_name>’ at site ‘<site_name>’ has not changed its state since <time_span>.” Checks the state of the door signal for a long time period of vehicle operation (> 48h). The state is determined even if the vehicle occasionally is switched off.	Doors (client and master PCU)	Check whether the door signal works as expected. If the door is out of order or locked, you can disable the diagnostics for this door to prevent unnecessary messages.
20.0.12 (Warning)	Warning	“Sensor <sensor_of_the_door> from door '<door_name>' at site '<site_name>' did not count any valid event since <time_span>.” Checks the signals sent from the sensor for a long time period of vehicle operation (> 48h). The state is determined even if the vehicle occasionally is switched off.	Doors (client and master PCU)	Check the concerned sensor (replace it, if necessary). Check whether the door is out of order and no counting events can be created. In this case you can disable the diagnostics for this door to prevent unnecessary messages.

DLX3 Identification ModuleID. SubModuleID. MessageID (Category)	Log Level	Log Message and Description	Activated with configuration of:	Measure
20.0.20 (Warning)	Warning	“Door '<door_name>' at site '<site_name>' opened while vehicle is driving.” Checks door signals when „vehicle moves“- status (calculated by PCU) is active.	Doors (client and master PCU)	Check if door signal and „vehicle moves“-status work as expected. In this case you can disable the diagnostics for this door to prevent unnecessary messages.
11.1.0 (Error)	Error	“No impulses at the odometer signal input while vehicle is driving.” Compares the speed calculated from odometer counts with GPS-speed.	Vehicle signals (master PCU)	Check, whether the odometer signal works correctly. Check whether the odometer’s calibration (pulses per kilometer) is configured correctly.
11.1.1 (Error)	Error	“Driving signal is inactive while vehicle is driving.” Compares the ‘vehicle in motion’ signal state with GPS-speed.	Vehicle signals (master PCU)	Check, whether the ‘vehicle in motion’ signal works correctly.
11.1.2 (Error)	Error	“Doors released while vehicle is driving.” Compares any ‘door release’ signal state with the ‘Vehicle driving’ state of the vehicle (calculated by the PCU).	Vehicle signals (master PCU)	Check, whether the ‘door release, left’ or ‘door release’ signal works correctly.
11.1.3 (Error)	Error	“Continuous impulses at the odometer signal input while vehicle stands still. Compares the speed calculated from odometer counts with GPS-speed.	Vehicle signals (master PCU)	Check, whether the odometer signal works correctly. Check whether the odometer’s calibration (pulses per kilometer) is configured correctly.
11.1.4 (Error)	Error	“Driving signal is active while vehicle stands still. Compares the ‘vehicle in motion’ signal state with GPS-speed.	Vehicle signals (master PCU)	Check, whether the ‘vehicle in motion’ signal works correctly.

DLX3 Identification ModuleID. SubModuleID. MessageID (Category)	Log Level	Log Message and Description	Activated with configuration of:	Measure
11.1.5 (Error)	Error	"'At stop' signal is active while vehicle is driving." Compares the 'vehicle at regular stop' signal state with the GPS-speed.	Vehicle signals (master PCU)	Check, whether the 'vehicle at regular stop' signal works correctly.

Table 53: Diagnostic Messages

Entry	Description
<site_name>	**Site Or Vehicle Name** of the PCU as configured in the PCU's **Configuration > System > General** page (see chapter 3.5).
<door_name>	**Identifier** of the door as configured in the PCU's **Configuration > System > Doors** page (see section 3.7).
<signal_number>	Number of the **Door Contact (1 or 2)** of the door as configured in the PCU's **Configuration > System > Doors** page (see section 3.7).
<sensor_of_the_door>	Number of the **Sensor (1…12)** (G1) **or (1…16)** (G2) of the door's **Sensor Bar** as configured in the PCU's **Configuration > System > Doors** page (see section 3.7). See page 17 for information about the groups G1 and G2.
<time_span>	Duration of the state in hours, minutes, seconds, days, months, years.

Table 54: Explanation of the variable content of Diagnostic Messages

The warnings described in table no. 52 can be activated or deactivated completely for the diagnosis per door.

Warnings 20.0.10, 20.0.11, 20.0.12 are recorded for the first time after a period of 48 hours. If the error is still existing, the warnings are reported again after a period of 48 hours.

Times for warnings 20.0.8, 20.0.10, 20.0.11 and 20.0.12 are reset when the error conditions is repealed.

Warning 20.0.20 is reset when error did not occur for 1000s.

5.6 Maintaining Client PCUs

As described in chapters 3.5 and 3.19 there can be client PCUs associated to a master PCU. On the **Device State > Device Information** page of the master PCU the client PCUs currently associated to the master are displayed:

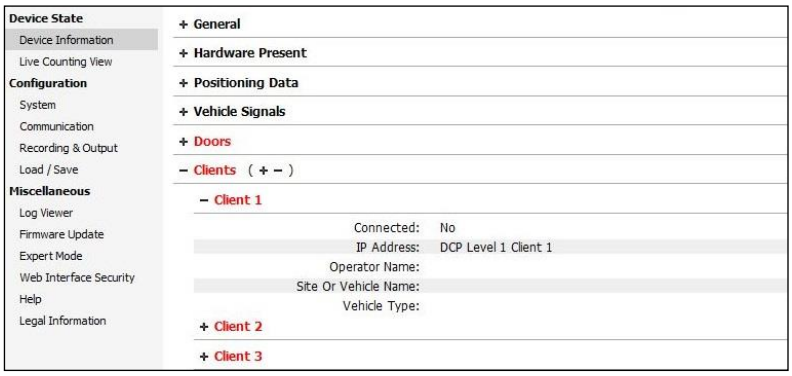


Figure 122: View of the current associated client PCUs

The following properties of the client are shown:

Property	Description
Connected	Always **Yes**. Exception: The client is configured as permanently connected and it is currently not associated (**No**).
IP Address	IP address of the client. It is displayed as a hyperlink. Click on the hyperlink to open the web interface of the client PCU.
Operator name	Operator name configured in the client PCU.
Site or vehicle name	Site or vehicle name configured in the client PCU.
Vehicle type	Vehicle type configured in the client PCU.
Error	Indicates whether the client PCU is in an error state or not.

Table 55: Device Information – Displayed information for a client PCU

Note: If the client PCU is configured as permanently connected and the client PCU is currently not associated to the master PCU, the values **IP Address**, **Operator Name**, **Site Or Vehicle Name**, and **Vehicle Type** are determined by the configuration of the master PCU as configured on the page **Configuration > System > Clients**.

5.7 Testing GSM/GPRS Communication

To check whether a GSM/GPRS connection is established please open the page **Device State > Device Information**. If the connection is established, the GSM provider ID is shown.

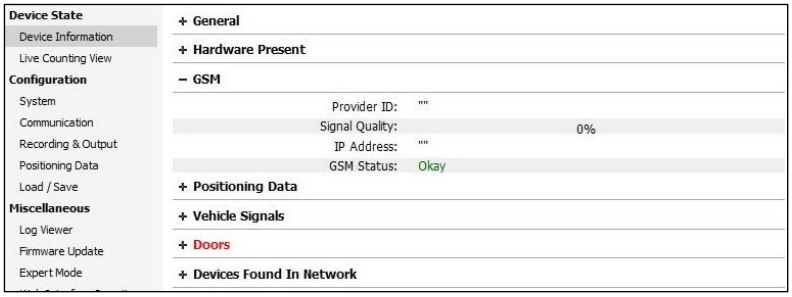


Figure 123: Testing the GSM status

You must force a GSM/GPRS connection because the models of the PCU-200 series support a GPRS connection on demand only. To do this, execute an FTP client test that will generate a test file, establishes a GSM/GPRS connection and sends the test file via FTP. Detailed information about the FTP client test can be found in chapter 5.10.

If the PCU detects an error when initializing the GSM module (e.g. invalid SIM-pin, etc.), a corresponding error message occurs at **Modem Status**.

If there are GSM/GPRS communication problems go to the page **Miscellaneous > Log Viewer**. Check the log entries of the modules:

pppmgr

pppd

chat

Errors are reported there.

Note: When **Modul not present** is shown at **GSM** in the **Hardware Present** area, then the PCU cannot communicate via GSM/GPRS. You can re-activate the function by shortly interrupting power supply to the PCU.

5.8 Scan for available Wi-Fi Network Stations

The PCU can search for available Wi-Fi network stations (access points) depending on its location. To do this, open the page **Configuration > Communication > Wi-Fi**.

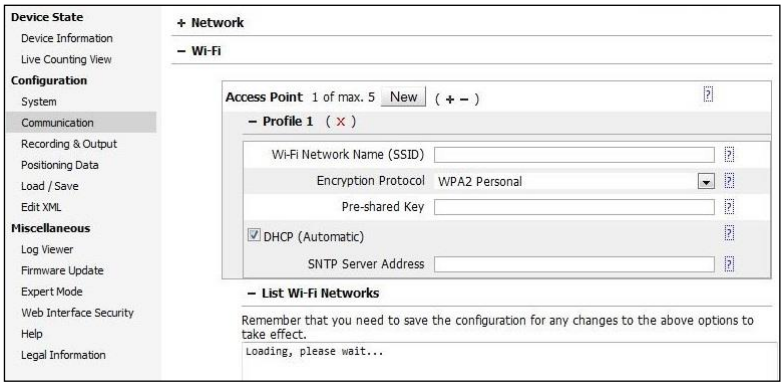


Figure 124: Scanning for available Wi-Fi network stations

Press the **List Wi-Fi Networks** button.

Wait until the list appears below the button.

5.9 Testing Wi-Fi Communication

To check whether a Wi-Fi connection is established, please open the page **Device State > Device Information**. If the connection is established, the "Wi-Fi SSID" and the "Wi-Fi IP address" are shown:

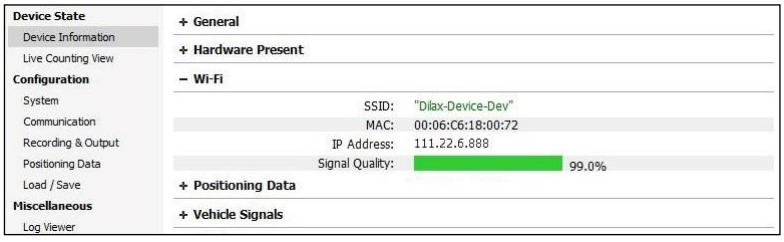


Figure 125: Testing the Wi-Fi status

When Wi-Fi communication problems occur open the page **Miscellaneous > Log Viewer**. Check the log entries of the modules:

wifimrg

wificonf

inetmgr

Errors are reported there.

5.10 Testing FTP Client Configuration

The configured FTP client configuration can be tested in the FTP server and client configuration (page **Configuration > Communication > FTP Client Configuration**).

1. Press the button **Start FTP Transmission Now**. A message box appears:

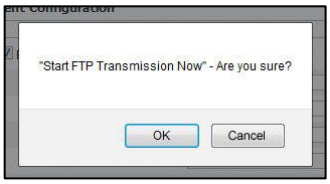


Figure 126: Confirm to start testing

2. Press **OK** to continue with testing.

A status information appears:

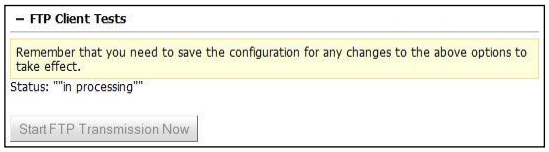


Figure 127: Transmission of a test file via FTP (processing)

The system transmits a test file to the remote FTP server. This can take some minutes, especially if the file is transferred via GPRS. When the transmission is finished a message will appear, if necessary an error message.

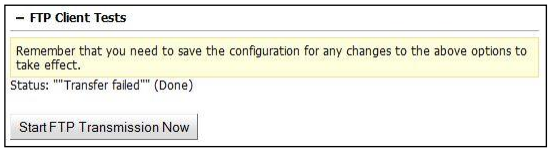


Figure 128: Transmission of a test file via FTP (done)

If the status message shows an error open the page **Miscellaneous > Log Viewer** and check the following modules for error messages:

- inetmgr
- putftp

5.11 Testing SMTP Configuration

The SMTP configuration can be tested on the **Configuration > Communication > SMTP** page.

1. Press the button **Start SMTP Transmission Now**. A message box appears.

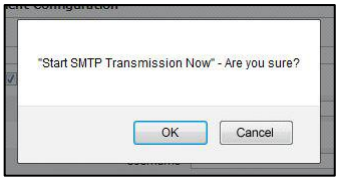


Figure 129: Confirm transmission of test data via SMTP

2. Press **OK** to continue with testing.

A status information appears.

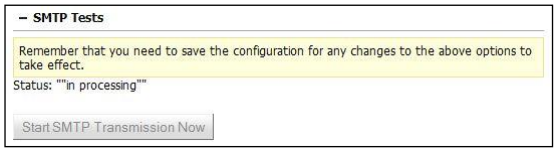


Figure 130: Transmission of test data via SMTP (processing)

The system transmits test a data file to the remote SMTP server. This can take some minutes, especially if the data is transferred via GPRS and the GPRS connection must be established before sending. When the transmission is finished, a message will appear, if necessary an error message.

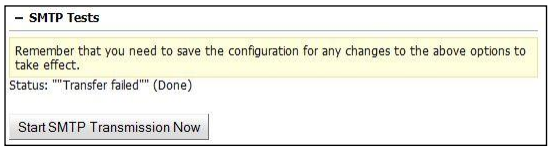


Figure 131: Transmission of a test data via SMTP (done)

If the status message shows an error, open the page **Miscellaneous > Log Viewer** and check the following modules for error messages:

- inetmgr
- smtp
- pppd

5.12 Testing HTTP Client Configuration

The HTTP client configuration can be tested on the page **Configuration > Communication > HTTP Client**.

1. Press the button **Start Connection Test**. A message box appears.

Figure 132: Confirm transmission of test data via HTTP

2. Press **OK** to continue with testing.

A status information appears.

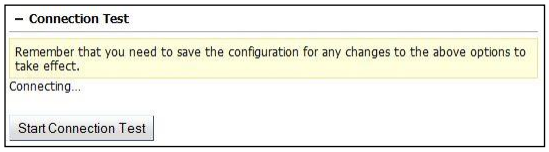


Figure 133: Transmission of test data via HTTP (processing)

The system transmits test a data file to the remote HTTP server. This can take some minutes, especially if the data is transferred via GPRS and the GPRS connection must be established before sending. When the transmission is finished, a message will appear, if necessary an error message.

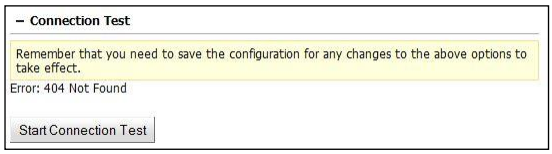


Figure 134: Transmission of a test data via HTTP (done)

If the status message shows an error, open the page **Miscellaneous > Log Viewer** and check the following module for error messages:

- inetmgr

5.13 Testing IBIS Communication

If there are IBIS communication problems open the **Configuration > System > General** page, set the **Logging Level** to "debug" and save this configuration.

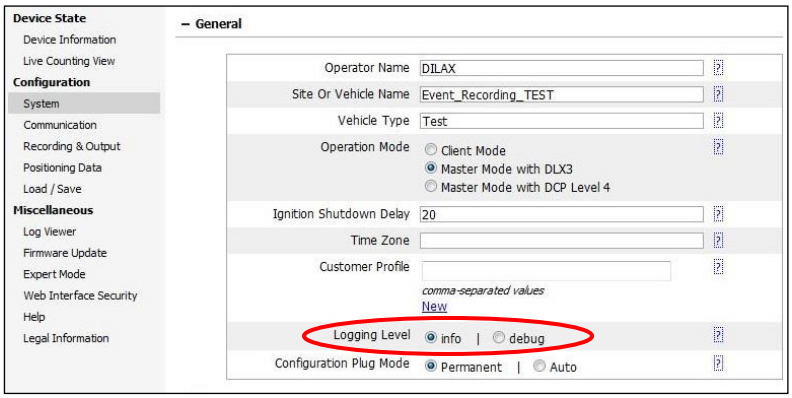


Figure 135: Setting the logging level to test IBIS communication

Now open the page **Miscellaneous > Log Viewer** and check the log entries of the module ibis. The received telegrams as well as errors are reported there.

5.14 Checking the odometer pulses calibration

The configuration of the odometer pulse signal is done at **Configuration > System > Vehicle Signals** (see chapter 3.9). The configuration mask must contain a value in the **Odometer Pulses Per Km** field so that the system is able to convert odometer pulses into a distance. As an exception, when the value cannot be determined from vehicle data, the automatic calibration can be used by entering the value "auto". The automatic calibration is a gradual process at which the value for pulses per kilometer converges from a start value to a nominal value. The current status of this procedure can be checked at **Device State > Device Information > Vehicle Signals > Odometer Details**.

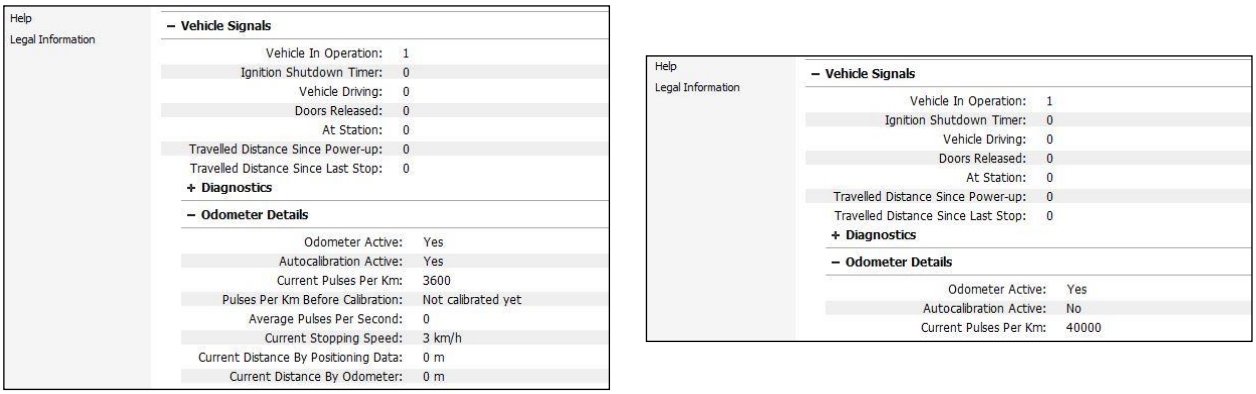


Figure 136: Odometer details (left: automatic calibration, right: when a value is configured)

Value	Description
Odometer Active	Yes: An odometer input has been configured. No: No configured odometer input. Configuration is done at **Configuration > System > Vehicle signals** (see chapter 3.9).
Autocalibration Active	Yes: **Odometer Pulses Per Km** input field has been configured with value "auto". No: **Odometer Pulses Per Km** input field contains a value. Configuration is done at **Configuration > System > Vehicle signals** (see chapter 3.9).
Current Pulses Per Km	Value used for distance calculation. The value entered into the **Odometer Pulses Per Km** input field at **Configuration > System > Vehicle Signals** (see chapter 3.9). The calibration result when automatic calibration is in process.
Pulses Per Km Before Calibration	Only visible in case of automatic calibration Start value of calibration. It will automatically be reset at each system start.
Average Pulses Per Second	Only visible in case of automatic calibration Number of pulses within the last second.
Current Stopping Speed	Only visible in case of automatic calibration Threshold value for stopping speed derived from the **Current Pulses Per Km** value.
Current Distance By Positioning Data	Only visible in case of automatic calibration Calibration distance of the current calibration cycle calculated from the GPS velocity. This value will only be increased in case of an approximate uniform movement and it will be reset after each cycle.

Value	Description
Current Distance By Odometer	Only visible in case of automatic calibration Calibration distance of the current calibration cycle calculated from the pulses of the odometer signal. This value will only be increased in case of an approximate uniform movement and it will be reset after each cycle. In calibrated state, this value must approximately meet the **Current Distance By Positioning Data** value.

5.15 Trouble Shooting Guide

An active LED "ERR" during operation indicates an error. Certain errors are associated with an error code. If such an error occurs, it is not only logged to the system log of the PCU but also displayed in the form of Morse code on the red error LED. The error code is repeated periodically. The following table gives an overview of the error codes:

Error code	Morse code (– long flash, ▪ short flash)	Description
0	– – – – –	IP address conflict at the Ethernet interface.
1	▪ – – –	Door not responding.
2	▪ ▪ – – –	Not enough sensors connected to the SSL bus.
3	▪ ▪ ▪ – –	Flickering sensor. A sensor flickers if it detects at least 1400 objects per minute when the door is open.
4	▪ ▪ ▪ ▪ –	General SSL bus failure.
5	▪ ▪ ▪ ▪ ▪	General sensor failure.
6	– ▪ ▪ ▪ ▪	Stored configuration file contains errors. The detailed error message can be found in the system log.
7	– – ▪ ▪ ▪	SSL-digital input failure.
8	– – – ▪ ▪	Blocked sensor. A sensor is blocked when an object stays continually within the sensor's range for at least 1 hour (5 hours if there is no associated door contact). The time is only counted if the door is open. If no door contact is configured a door is open by definition.
9	– – – – ▪	The device is in fail-safe mode. See chapter 5.1 of a description of this operation mode.

Table 56: Morse codes of the error LED

When the device is powered up the error LED is active and will remain active for a short period until the firmware has been bootstrapped. This does not indicate an error.

The following table explains possible problems and their solutions:

Problem	Possible cause	Solution
PWR LED is off.	PCU has no power supply	Check cabling and connections, pinning of connector X03.
	PCU defective	Replace PCU.
ERR LED always on.	PCU defective	Replace PCU.
ERR LED flashing error code 0.	Another PCU has the same IP address.	Change the IP address of the other PCU and restart it.
ERR LED flashing error code 1.	Door not responding.	Check whether all client PCUs are working.
ERR LED flashing error code 2.	Not enough sensors connected to the SSL bus.	Check SSL bus cabling and sensors.
ERR LED flashing error code 3.	Flickering sensor. A sensor flickers if it detects at least 1400 objects per minute when the door is open.	Check sensor/sensor Product Manual.
ERR LED flashing error code 4.	General SSL bus failure.	Check sensor/sensor Product Manual.
ERR LED flashing error code 5.	General sensor failure.	Check sensor/sensor Product Manual.
ERR LED flashing error code 6.	The stored configuration file contains errors. The detailed error message can be found in the system log.	Check configuration file for errors and correct. The configuration file have to be replaced.
ERR LED flashing error code 7.	SSL-digital input failure.	Check digital input INP-450.
ERR LED flashing error code 8.	Blocked sensor.	Check sensor/sensor product Manual.
Digital Input on PCU not working.	No Voltage supplied to the digital input between IN+ and the respective INx- (IN0-, IN1- or IN3-).	Check cabling, external switching contact and voltages at PCU (min. and max. Voltages for switching).
	Digital input of PCU defective.	Replace PCU.

Problem	Possible cause	Solution
Web interface for configuration cannot be displayed.	Ethernet cable not connected.	Check cables and connection. ACT LED is flashing when there is traffic.
	PCU setup for DHCP and not connected to a DHCP server.	Make sure PCU is connected to a DHCP capable server or disable DHCP in PCU. You can install a DHCP server e.g. TFTPD32.
	PCU not in same network.	Make sure PCU and the connecting PC are in the same network.
	Ethernet interface of PCU defective.	Replace PCU.
SSL bus not working, sensors are missing.	SSL cable is not connected or defective.	Check cables and connection from PCU to first sensor and between all sensors. Make sure cable lengths are according to specifications.
	Sensor connectors defective.	Swap the sensors and look for senor function to find the defect sensor. Replace the defect sensor.
	Sensors are missing, ERR LED is flashing error code 2.	Check cables and connections between sensors, check error log and replace defective cable or sensor (see Sensor Product Manual).
Counting direction is reversed.	Counting direction is inverted.	Check **Configuration > Doors** page of configuration and select the other option of **Invert** at the sensor bar.
Wi-Fi Module (Motorola) does not connect.	The status of the SSID toggles between "not connected" and "AP-SSID".	Check the correctness of pre shared key. The Motorola Wi-Fi module does not accept a colon in the pre shared key. Check if a colon is included.
Incorrect configuration file message on upload on configuration.	The name of the configuration file does not end with "config.xml".	Rename the configuration file to end with "config", e.g. "test_config.xml".
The PCU is not sending live data.	Wrong configuration, no connection to the mobile provider (when using GSM), the vehicle does not move, there is no valid time (missing time synchronization)	Check if the configuration of the HTTP client and if the GSM settings are correct and change them if necessary. Check if there is a valid time (date/time). The PCU generates und uses live data only when there was successful time synchronization. In case the vehicle has been configured that live data should only be generated when the vehicle is moving, move the vehicle.

Table 57: Trouble shooting

5.16 Resolving Ethernet Problems

Web browser

If you have trouble accessing the web interface refresh the page or restart the web browser.

Note: If it is still not possible to access the web interface, the Ethernet interface of the service PC may perhaps be the reason. Set the Ethernet interface of the service PC to 10Mbit/s.

Ping

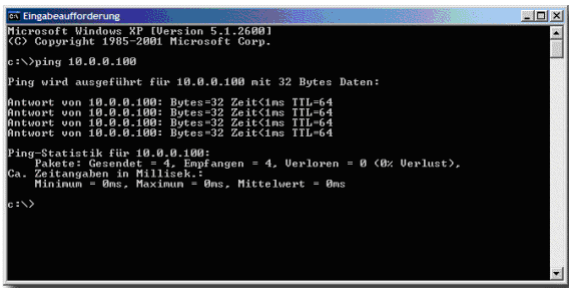


Figure 137: Screenshot of "ping"

To test the Ethernet connection of the PCU try to "ping" it from a PC in the same network. Operating systems like Microsoft Windows and GNU/Linux provide a program called "ping" to send and receive ICMP ping packets over IP.

Wireshark

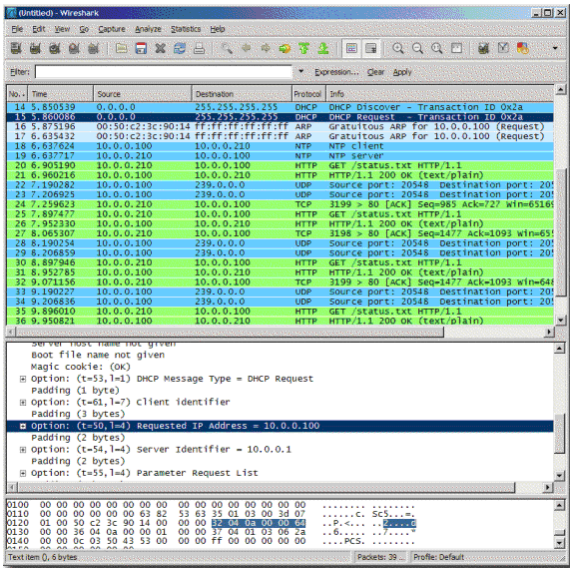


Figure 138: Screenshot of Wireshark

If there are network problems on a deeper level, it might be advisable to use a network sniffer/protocol analyzer, for example the "Microsoft Network Monitor" or the network sniffer tool "Wireshark". Both tools are free.

TFTPD32

TFTPD32 is a free server tool that can be installed at Microsoft Windows. It includes a DHCP server. You can use this tool to temporary install a DHCP server in the network. This is helpful when there is no DHCP server in the network but the Ethernet network interface of the PCU is configured for automatic configuration via DHCP (see chapter 3.6).

5.17 Expert Mode

The expert mode gives you full access to all internal data of the web interface. This may be necessary to solve configuration saving problems (see chapter 5.19).

Warning: Please only activate this mode if you have sufficient experience with the internal data structures and mechanism.

To start the expert mode open the page **Miscellaneous > Expert Mode > Expert Options**. The first three check boxes must be checked for full access:

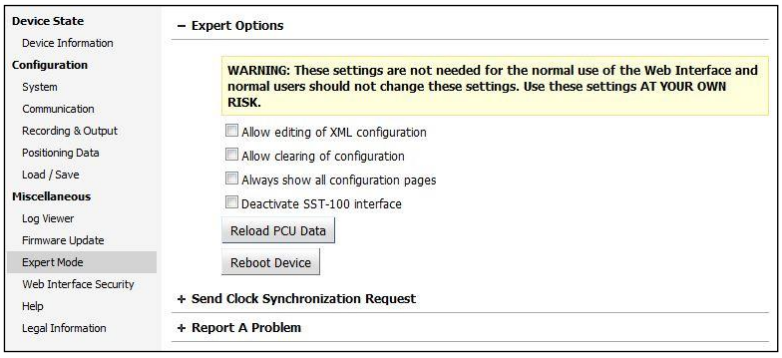


Figure 139: Starting the expert mode

The **Deactivate SST-100 interface** checkbox is for deactivating/activating the use of the interface to connect an SST-100. In this case, no SST-100 is required to operate/configure the PCU-200, despite an existing X12 connection (see Section 2.4.10). This deactivates the function of the SST-100 (see Section 4.3).

Caution: Activating/deactivating the SST-100 interface automatically restarts the device.

Manually synchronizing the device time

The devices system time can be set at the page **Miscellaneous > Expert Mode > Send Clock Synchronization Request**. With this function you can also set the system time manually (**Device Time** and **Time Zone**).

5.18 Resolving Configuration Saving Problems

If a new configuration cannot be saved and the message "... Unexpected attribute xmlns= ..." appears activate the expert mode to open the configuration file in an XML editor.

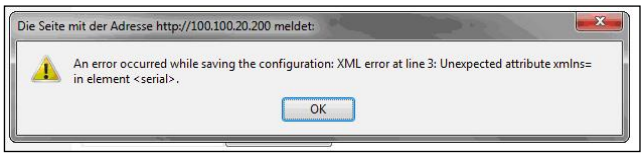


Figure 140: Error message during configuration saving

Execute the following steps:

1. Activate the expert mode.
2. Open the page **Configuration > Edit XML**. The configuration file is displayed in the XML editor:

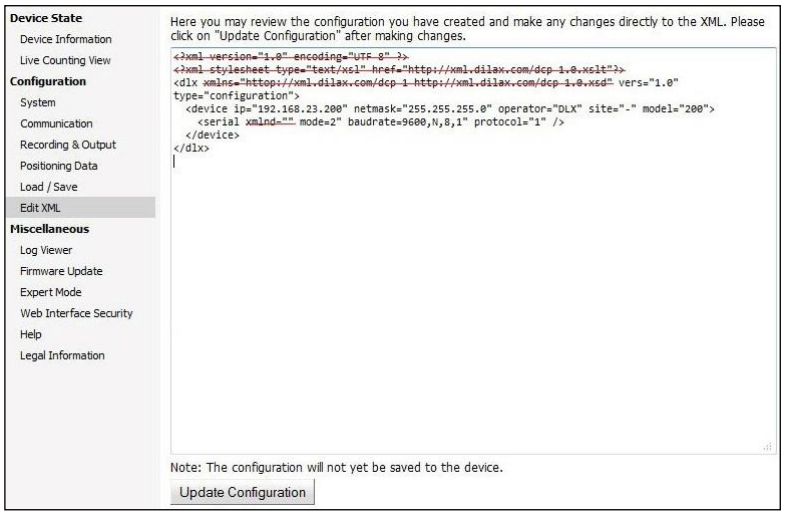


Figure 141: Lines which contain errors

3. Check if the file contains the lines which are crossed out in Figure 154.
4. Delete the crossed out lines directly in the XML editor.
5. Open the page **Configuration > Load / Save** and save the configuration.

5.19 Check current Hardware Configuration at Firmware Update

After a firmware update, it could be possible that the existing hardware configuration does no longer meet the required criteria. In that case, the hardware could change into safe mode (see chapter 5.1).

We recommend to check the configuration on a test device using the currently available firmware. Therefore, the test device should

- be identical to the device where the new firmware shall be installed,
- easily accessible; that means, no remote updates to react easily to errors and
- include the current firmware version.

The testing procedure is described in chapter 4.2.3. Realize configuration changes until testing of the test device was successful.
Refresh the changed valid configuration first on the device where the firmware shall be installed before performing the update.

6 Appendix

6.1 Technical Data PCU-200

6.1.1 Electrical Data

Nominal voltage	24 V_{DC}, 36 V_{DC}
Input voltage range	16.8 … 45 V_{DC} (min. pulse 14.4 V_{DC})
Current consumption @ 24 V_{DC}	up to 160 mA (no sensors) up to 550 mA (with 12 sensors, G1), up to 650 mA (with 16 sensors, G2) See page 17 for information about the groups G1 and G2.
Isolation	>1GOhm @ 500V
Voltage supply interruption class	S2

Table 58: Electrical data PCU-200

6.1.2 Mechanical Data

Dimensions (L x W x H)	IP40 housing: IP54 housing: IP40 rack housing:	108,8 x 144 x 48,6 mm 108,6 x 144 x 50,2 mm 111,8 x 128,4 (3 HE) x 50,5 (10 TE) mm
Weight	approx. 500g (for exact weights refer to the technical drawings of the devices)	

Table 59: Mechanical data PCU-200

6.1.3 Environmental Data

Operating temperature	-25°C - +70°C
Storage temperature	-40°C - +85°C
Relative humidity	95% (non-condensing)
Vibration and shock resistance	EN 61373 category 1, class B
EMC	EN 50121-3-2
Railway applications	EN 50155
Protection class	EN 60529 IP40 or IP54 (depends on unit type)
ECE R10 - E1	No. 036975

Table 60: Environmental data PCU-200

6.2 Counting Data Protocols

The models of the PCU-200 series can interact with various devices in an automatic counting system. To integrate a PCU in another counting system, some counting protocols have been developed for interaction with other components of a counting system.

6.2.1 Data Transmission over FTP

The PCU can transfer its counting data regularly to an FTP server. Data is transferred as files in DLX3 format.

6.2.2 DILAX Counting Protocol (DCP)

This protocol is used internally for communication between a master PCU and the client PCUs. Additionally, if a third party board computer implements this protocol it can deliver some signals to the PCU via network (like vehicle signals, system time or GPS information). Refer to the protocol specification for a description of the protocol level 2.

The level 3 push mode with JSON formatting is used for the Live Tracking function. Refer to the protocol specification for a description of the protocol level 3.

6.2.3 J1587 (J1708)

A third party onboard unit can request counting data by means of the J1587 application layer protocol. The physical and data link layer defined in the J1708 standard is used for the communication.

6.3 Timing Characteristics

The following table describes typical timings used by PCU communication services. It is determined between the following connections modes:

- GSM connection (see chapters 2 and 3.11)
- Wi-Fi or Ethernet connection (see chapters 2, 3.6 and 3.20)

Service	GSM connection	Wi-Fi/Ethernet connection
FTP		
Looking for files to be transferred by the FTP service	5 s	
Transferring files via FTP timeout	2 min	1 min
Checking for instruction file at FTP server (see 4.4.2)	1 h	15 min
Execution of available instruction file (see 4.4.2) if PCU is running in Client mode every if PCU is running in Master mode	 5 min Immediately	
SMTP		
Looking for e-mails to be transferred by SMTP service after startup and then every	 15 min 1 h	 2 min 60 s
Transferring e-mails via SMTP timeout	1 h	30 min
HTTP		
Looking for files to be transferred by HTTP service		

every	10 s	
in case of an transmission error	15 s	
in case of 10 consecutive transmission errors	90 s	
Data Recording		
Looking for raw data to be compressed	60 s	
Looking for raw data to be prepared for transmission every	3 min	
GSM		
If configured to run in on-demand mode terminating PPP active connection after	60 min	not applicable
Active PPP server connection will be refreshed every	15 min	not applicable

Table 61: Timing characteristics used by PCU communication services

6.4 Drawings

(All values in millimeters.)

Note: The drawings of the PCU-250 model are shown. Connectors may vary depending on model and variant.

IP40 surface-mounted housing (metal shell)

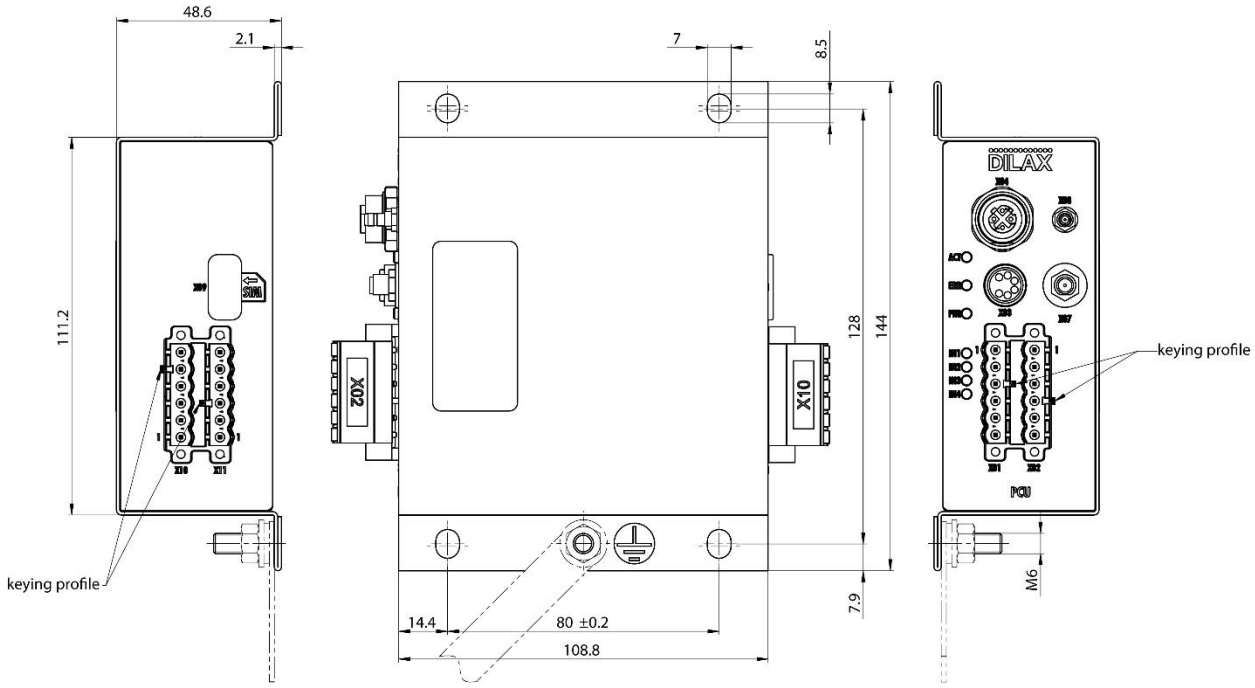


Figure 142: Drawing PCU-200 IP40 surface-mounted housing (metal shell)

IP54 surface-mounted housing

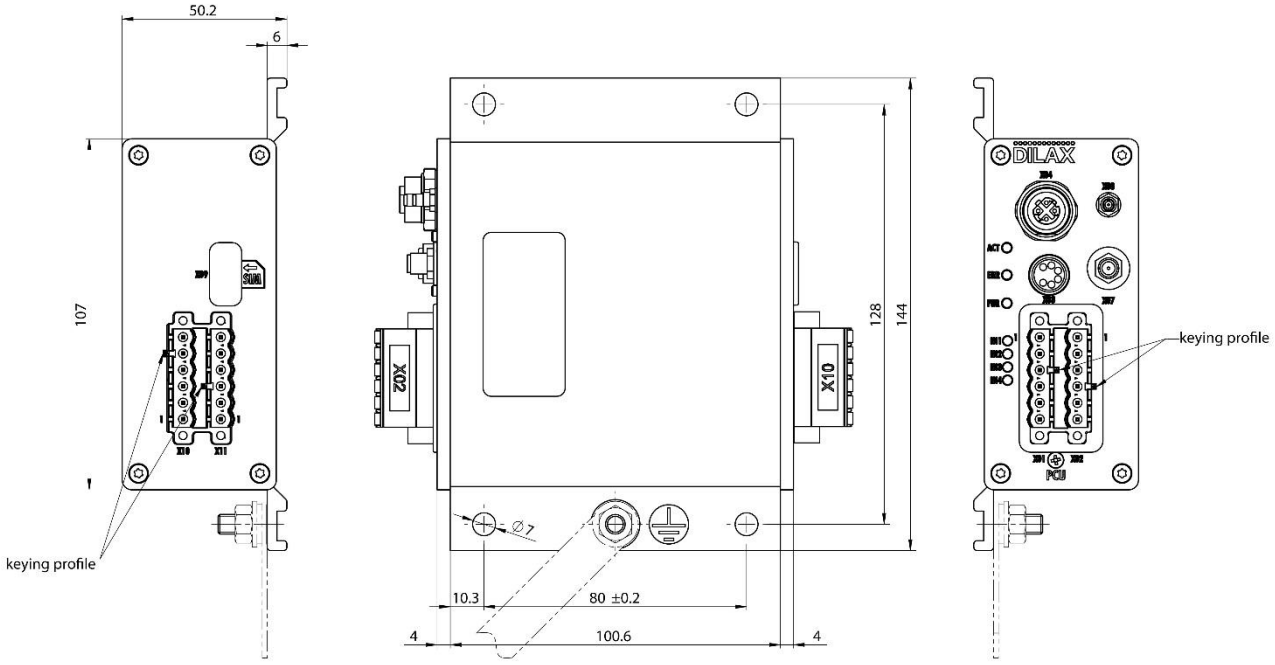


Figure 143: Drawing PCU-200 IP54 surface-mounted housing

IP40 rack housing

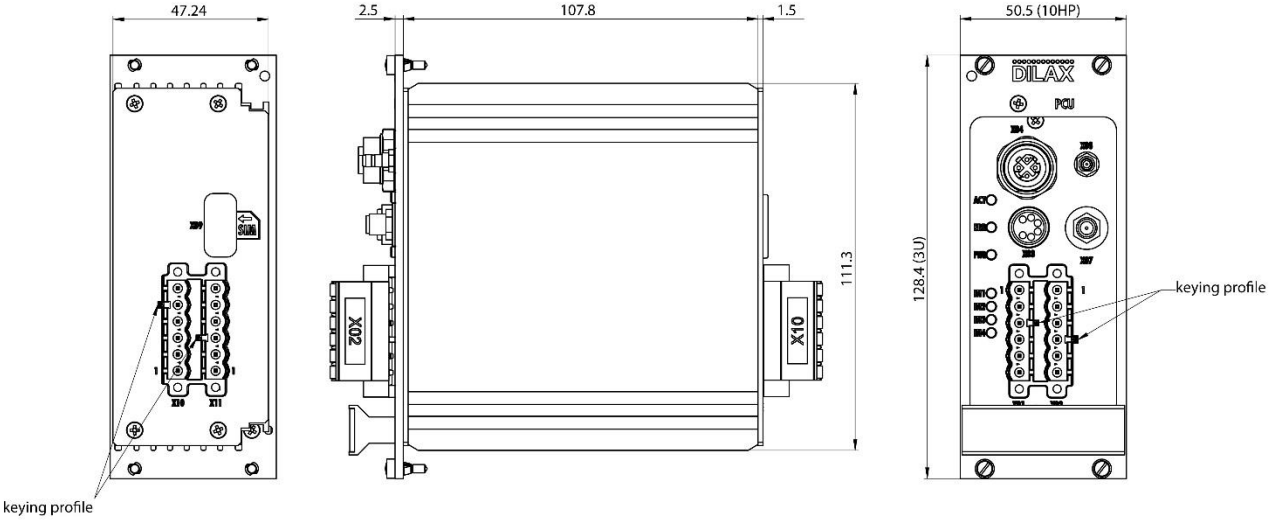


Figure 144: Drawing PCU-200 IP40 rack housing

6.5 Block Diagram

The models of the PCU-200 series consist of several circuit blocks. Core is a 32-bit ARM processor with SDRAM and Flash memory. The power supply block converts the input voltage to the different voltages needed in the PCU.

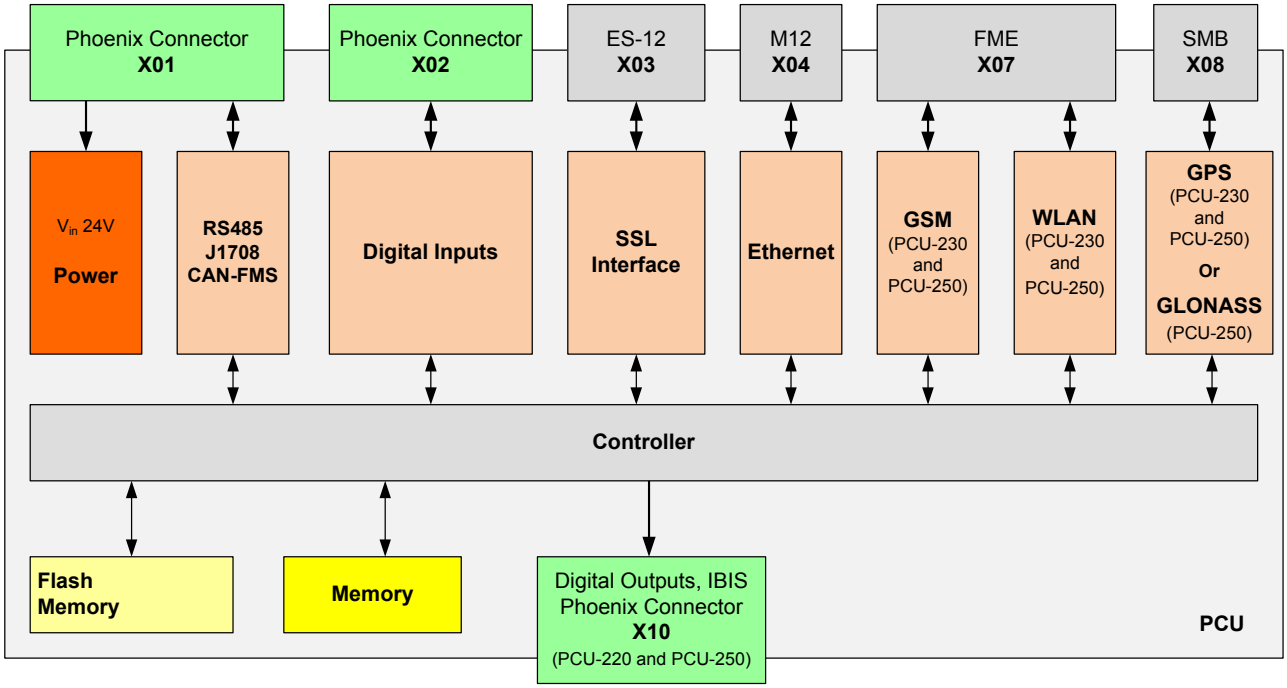


Figure 145: Block diagram

7 Glossary of Acronyms and Abbreviations

Acronym/Abbreviation	Description
3GPP	3rd Generation Partnership Project: unites telecommunications standards bodies – as Organizational Partners
3G	3rd Generation of mobile telephone system
AC	Alternating Current
APC	Automatic Passenger Counting
ARP	Address Resolution Protocol
CSV	Comma Separated Value
C-plug	Configuration plug
DC	Direct Current
DCP	DILAX Counting Protocol, the successor of the DILAX LAN protocol
DCP L1	DILAX Counting Protocol Level 1 (RS485 based)
DCP L2	DILAX Counting Protocol Level 2 (UDP/IP based)
DCP L3	DILAX Counting Protocol Level 3 (TCP/IP and HTTP based)
DCP L4	DILAX Counting Protocol Level 4 (FTP based)
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DRP	DILAX Realtime Protocol (communication protocol for live data, DCP L3 based)
DSN	DILAX Simple Network (1-wire based communication protocol for ESL)
ESL	Extended Sensor Link (additional sensor data bus for external sensors, e.g. temperature sensors
FTP	File Transfer Protocol
GPRS	General Packet Radio System
GPS	Global Positioning System
GSM	Global System for Mobile Communications
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IBIS	Integrated On-Board Information System (specified by VDV 300)
J1708	Serial data communications between microcomputer systems in heavy duty vehicle applications. The protocol was designed by the Society of Automotive Engineers (SAE).
PCM	Passenger Counting Master
NMEA	National Marine Electronics Association (GPS data format)
PCU	Passenger Counting Unit
PEM	Privacy Enhanced Mail, file format to store keys and certificates
PPP	Point to Point Protocol

Acronym/Abbreviation	Description
RSA	Ron Rivest (see also http://en.wikipedia.org/wiki/Ron_Rivest), Adi Shamir (see also http://en.wikipedia.org/wiki/Adi_Shamir), and Leonard Adleman (see also http://en.wikipedia.org/wiki/Leonard_Adleman), public-key cryptography
SAE	Society of Automotive Engineers
SNTP	Simple Network Time Protocol
SSL	Serial Sensor Link
TBD	to be determined
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunications System
Wi-Fi	Wi-Fi is a trademark of the Wi-Fi Alliance for WLAN devices

Table 62: Glossary