Ethernet Cable Guard

Manual

Version 1 | 30.1.2024 | for firmware V1.04 and above

Order numbers: 700-200-LAN01

Link to newest version of manual

Helmholz GmbH & Co. KG | Hannberger Weg 2 | D-91091 Großenseebach | Germany
Phone +49 9135 7380-0 | Fax +49 9135 7380-110 | info@helmholz.de | www.helmholz.com

Notes

All rights reserved, including those related to the translation, reprinting, and reproduction of this manual or of parts thereof.

No part of this manual may be reproduced, processed, duplicated, or distributed in any form (photocopy, microfilm, or any other methods), even for training purposes or with the use of electronic systems, without written approval from Helmholz GmbH & Co. KG.

All rights reserved in the event of the granting of a patent or the registration of a utility model.

To download the latest version of this manual, please visit our website at www.helmholz.de.

We welcome all ideas and suggestions.

Copyright © 2024 by

Helmholz GmbH & Co. KG

Hannberger Weg 2 | 91091 Großenseebach

All trademarks shown or mentioned in this document are the property of their respective owners or manufacturers. The representation and naming serve exclusively to explain the use and setting options of the products documented here.

Revision Record:

Version	Date	Change
1	29.1.2024	First version for Firmware V1.04

Contents

1 General 5

1.1 Structure of the manual 5

1.2 Target audience for this manual 5

1.3 Safety instructions 5

1.4 Note symbols and signal words 6

1.5 Intended use 7

1.6 Improper use 7

1.7 Liability 8

1.7.1 Disclaimer of liability 8

1.7.2 Warranty 8

1.8 Open Source 8

2 Security recommendations 9

3 How the Cable Guard works 11

3.1 Design of the Cable Guard 11

4 Installation and removal 12

4.1 Access restriction 12

4.2 Mounting and minimum distances 12

4.3 Electrical installation 12

4.4 Protection against electrostatic discharges 12

4.5 EMC protection 13

4.6 Operation 13

4.7 Recycling / WEEE 13

5 Preparing the Cable Guard 14

5.1 Power supply 14

5.2 Connection of the line to be monitored (DATA) 14

5.3 Connecting the data connection (LAN) 14

5.4 Connecting the digital outputs (Q1/Q2) 15

6 Initial Startup ("Teach-In") 16

6.1 Display of the operating statuses via the LEDs 17

7 Configuration and diagnostics via the web interface 18

7.1 Access to the website 18

7.2 Main view 19

7.3 Configuration 20

7.3.1 Basic configuration "Settings" ... 20

7.3.2 Ethernet configuration (LAN) ... 20

7.3.3 Sending the cable status via MQTT ... 21

7.4 Firmware Update ... 22

7.5 Factory Reset ... 23

8 FAQ ... 24

9 Technical data ... 27

1 General

This operating manual applies only to devices, assemblies, software, and services of Helmholz GmbH & Co. KG.

1.1 Structure of the manual

This manual is divided into 10 sections.

Section 1 contains **general information** and **safety instructions**.

Section 2 refers to **Security Recommendations**.

Section 3 explains **how the Cable Guard works and where it is used**.

Section 4 explains the **installation and removal**.

Section 5 shows the **initial hardware commissioning**

Section 6 explains the **first setup** of the Cable Guard

Section 7 describes the **configuration options**, **firmware update** and **factory reset**

A detailed FAQ ("Frequently asked questions") can be found in section 8

The **technical data** of the device is listed in section 9

1.2 Target audience for this manual

This description is only intended for trained personnel qualified in control and automation engineering who are familiar with the applicable national standards. For installation, commissioning, and operation of the components, compliance with the instructions and explanations in this operating manual is essential.

WARNING

Configuration, execution, and operating errors can interfere with the proper operation of the device and result in personal injury, as well as material or environmental damage. Only suitably qualified personnel may operate the devices!

Qualified personnel must ensure that the application and use of the products described meet all the safety requirements, including all relevant laws, regulations, provisions, and standards.

1.3 Safety instructions

The safety instructions must be observed to prevent harm to living creatures, material goods, and the environment. The safety notes indicate possible hazards and provide information about how hazardous situations can be prevented.

1.4 Note symbols and signal words

HAZARD

If the hazard warning is ignored, there is an imminent danger to life and health of people from electrical voltage.

WARNING

If the warning is ignored, there is a probable danger to life and health of people.

CAUTION

If the caution note is ignored, people can be injured or harmed.

ATTENTION

Draws attention to sources of error that can damage equipment or the environment.

NOTE

Gives an indication for better understanding or preventing errors.

1.5 Intended use

The Ethernet Cable Guard (hereinafter referred to as "the device") can be used to monitor 100 MBit Ethernet data lines.

All components are supplied with a factory hardware and software configuration. The user must carry out the hardware and software configuration for the conditions of use. Modifications to hardware or software configurations which are beyond the documented options are not permitted and nullify the liability of Helmholz GmbH & Co. KG.

The device may not be used as the only means for preventing hazardous situations on machinery and systems.

The Ethernet Cable Guard cannot be used for a direct connection to the Internet. Always use a dedicated router with a sufficiently dimensioned Internet firewall for an Internet connection. Observe the security recommendations for project planning, use and maintenance.

Problem-free and safe operation of the device presumes proper transport, storage, setup, assembly, installation, commissioning, operation, and maintenance.

The ambient conditions provided in the technical specifications must be adhered to.

The device has a protection rating of IP20 and must be installed in an electrical operating room or a control box/cabinet to protect it against environmental influences. To prevent unauthorized access, the doors of control boxes/cabinets must be closed and possibly locked during operation.

1.6 Improper use

WARNING

The consequences of improper use may include personal injuries of the user or third parties as well as property damage to the control system, the product, or the environment.
Use the device only as intended!

1.7 Liability

The contents of this manual are subject to technical changes resulting from the continuous development of products of Helmholz GmbH & Co. KG. If this manual contains technical or clerical errors, we reserve the right to make changes at any time without notice.

No claims for modification of delivered products can be asserted based on the information, illustrations, and descriptions in this documentation. Beyond the instructions contained in the operating manual, the applicable national and international standards and regulations must also be observed in any case.

1.7.1 Disclaimer of liability

Helmholz GmbH &Co. KG is not liable for damages if these were caused by use or application of products that was improper or not as intended.

Helmholz GmbH & Co. KG assumes no responsibility for any printing errors or other inaccuracies that may appear in the operating manual unless there are serious errors about which Helmholz GmbH & Co. KG was already demonstrably aware.

Beyond the instructions contained in the operating manual, the applicable national and international standards and regulations must also be observed in any case.

Helmholz GmbH & CO. KG is not liable for damage caused by software that is running on the user’s equipment which compromises, damages, or infects additional equipment or processes through the remote maintenance connection and which triggers or permits unwanted data transfer.

1.7.2 Warranty

Report any defects to the manufacturer immediately after discovery of the defect.

The warranty is not valid in case of:

- Failure to observe these operating instructions
- Use of the device that is not as intended
- Improper work on and with the device
- Operating errors
- Unauthorized modifications to the device

The agreements met upon contract conclusion under “General Terms and Conditions of Helmholz GmbH & Co. KG” apply.

1.8 Open Source

Among other things, our products contain open-source software. This software is subject to the relevant license terms. The relevant license terms, including a copy of the full license text, are downloadable from the product website. They are also provided in our download area of the respective products at www.helmholz.de.

Furthermore, we offer to send the complete corresponding source code of the respective open-source software to you and to any third party as a DVD upon your request for a contribution towards expenses of Euro 10.00. This offer is valid for a period of three years. This offer is valid for a period of three years, calculated from the delivery of the product.

2 Security recommendations

Managed switches are network infrastructure components, and thus an important element in the security considerations of a system or network. When using the device, therefore please consider the following recommendations to prohibit unauthorized access to plants and systems.

General:

- Ensure at regular intervals that all relevant components fulfill these recommendations and possibly any other internal security guidelines.
- Evaluate your system holistically with a view to security. Use a cell protection concepts (“defense-in-depth”) with corresponding products, such as the WALL IE.
- Regularly inform yourself about security threats for all your components

Physical access:

- Limit physical access to components of relevance to security to qualified personnel.

Security of the software:

- Always keep the firmware of all communications components up to date.
- Inform yourself regularly of firmware updates for the product.
- Only activate protocols and functions you really need
- If possible, always use those variants of protocols that provide more security

Passwords:

- Define rules and roles for usage of the devices and the awarding of passwords
- Change standard passwords
- Only use strong passwords. Avoid weak passwords like, for example, “password1”, “123456789”, or similar.
- Ensure that all passwords are inaccessible to unauthorized personnel.
- Don’t use one password for various users and systems.

Helmholz is a member of the CERT@VDE. In addition to our technical newsletter, we communicate our security-relevant updates, patches and advisories to you as a user of Helmholz products. Find out more and use the services and database of the **CERT@VDE** to make your systems secure and keep them secure.

The Helmholz "**Product Security Incident Response Team**" **(PSIRT)** supports you proactively to protect your machines as best as possible in the context of industrial communication. Whenever new potential threats occur or are reported to us, we evaluate and process them immediately and provide you with recommended actions, patches and updates as quickly as possible to reduce the risk to a minimum.

You can help too: Report any product incidents to our **Product Security Incident Response Team** at psirt@helmholz.de or support@helmholz.de.

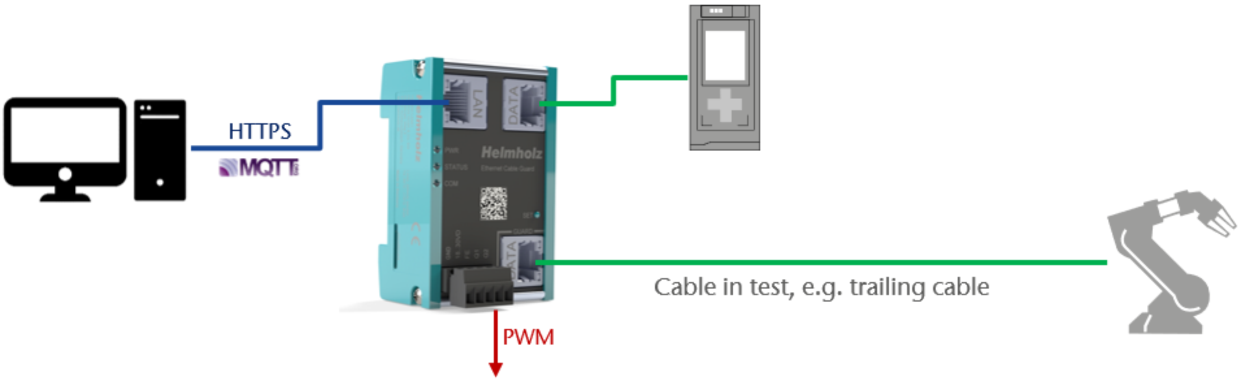
You can find more information on the topic of security here, for example:

- Helmholz PSIRT webpage
- CERT@VDE
- Sichere-industrie.de
- Bundesamt für Sicherheit in der Informationstechnik (BSI)
- Allianz für Cyber-Sicherheit

3 How the Cable Guard works

The Ethernet Cable Guard enables the service life monitoring of Ethernet data cables (100Base-TX) with a focus on dynamic applications in automation technology, such as a trailing cable to moving machine parts (robots). With the Ethernet Cable Guard, system availability can be increased, and downtimes can be planned. This enables a significant reduction in maintenance costs.

The Cable Guard is looped into the cable harness to be monitored and can provide information about the quality of the cable connection via a status LED, a separate network connection or a digital output. The feedback can be displayed as a PWM signal at the output. The alarm limit value can be set individually ("cable status" 99 - 50 %).



For integration into IIoT structures, the monitored cable status can also be sent via MQTT by the Cable Guard.

The compact design is suitable for use in decentralized control cabinets and can be mounted on standard DIN rails.

The Cable Guard is also suitable for EtherCAT, EtherNet/IP and 2-pair PROFINET applications.

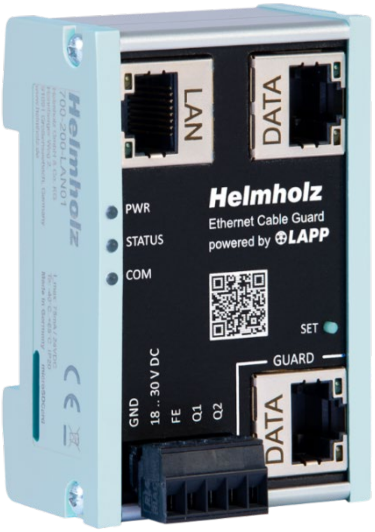
3.1 Design of the Cable Guard

The Cable Guard has two RJ45 connections (DATA) for the cable to be monitored and a LAN connection for configuration via the web interface and diagnostic queries.

The LEDs on the left edge of the housing indicate the status of the device (PWR / STATUS / COM) and the status of the monitored data line.

Various functions can be executed via the function button (SET).

Two additional 24V outputs for status information are available on the power supply connector.



4 Installation and removal

4.1 Access restriction

The modules are open operating equipment and must only be installed in electrical equipment rooms, cabinets, or housings.

Access to the electrical equipment rooms, cabinets, or housings must only be possible using a tool or key, and access should only be granted to trained or authorized personnel.

4.2 Mounting and minimum distances

The Ethernet Cable Guard can be mounted on a DIN rail and installed in any position. It is recommended to keep minimum distances when mounting. By keeping the minimum distances

- the modules can be mounted or dismantled without having to dismantle other parts of the system.
- there is enough space to connect all existing connections and contacting possibilities with commercially available accessories.
- There is space for any necessary cable routing.

ATTENTION

Installation must be carried out in accordance with VDE 0100/IEC 364 and applicable national standards. The device has protection level IP20. If a higher degree of protection is required, it must be installed in an enclosure or a control cabinet.

4.3 Electrical installation

Observe the regional safety regulations.

4.4 Protection against electrostatic discharges

To prevent damage through electrostatic discharges, the following safety measures are to be followed during assembly and service work:

- Never place components and modules directly on plastic items (such as polystyrene, PE film) or in their vicinity.
- Before starting work, touch the grounded housing to discharge static electricity.
- Only work with discharged tools.
- Do not touch components and assemblies on contacts.

4.5 EMC protection

To ensure electromagnetic compatibility (EMC) in your control cabinets in electrically harsh environments, the known rules of EMC-compliant configuration are to be observed in the design and construction.

ATTENTION

Observe all standards, regulations and rules regarding shielding when setting up the system and laying the necessary cables. Errors in the shielding can lead to malfunctions or even failure of the system.

4.6 Operation

Operate the device only in flawless condition. The permissible operating conditions and performance limits must be adhered to.

Retrofits, changes, or modifications to the device are strictly forbidden.

The device is a piece of operating equipment intended for use in industrial plants. During operation, all covers on the unit and the installation must be closed to ensure protection against contact

ATTENTION

When the Ethernet Cable Guard is switched off, bus connections are interrupted! Before starting any work on the device, make sure that no impermissible interference occurs in connected systems when the bus connections are interrupted.

4.7 Recycling / WEEE

The company Helmholz GmbH & Co. KG is registered as a manufacturer with the HELMHOLZ brand and the device type "Small devices of information and telecommunications technology for exclusive use in households other than private households" as well as the following registration data:

Helmholz GmbH & Co. KG,
Location / Headquarters: 91091 Großenseebach,
Address: Hannberger Weg 2,
Name of authorized representative: Carsten Bokholt,

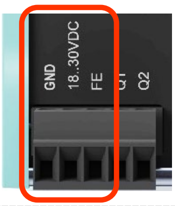
Registration number: **DE 44315750**

The electrical devices described in this document are to be recycled. According to Directive 2012/19/EU on waste electrical and electronic equipment (WEEE), they must not be disposed of by municipal waste disposal companies.

5 Preparing the Cable Guard

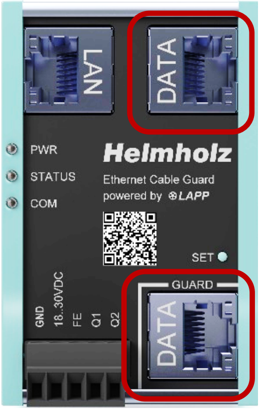
5.1 Power supply

The Cable Guard must be supplied with DC 18 ... 28 V via the supplied connector plug with DC 24 V.



NOTE

The housing of the Cable Guard is not earthed. Please connect the functional earth connection ("FE") of the switch properly to the reference potential.



5.2 Connection of the line to be monitored (DATA)

The Cable Guard has two "DATA" RJ45 connections for the link to be monitored.

The cable to be monitored (e.g. a trailing cable) must be connected to the lower connection ("Guard"). The upper DATA connection should then be connected to the communication partner (e.g. the control unit) using another standard industrial Ethernet cable.

The Cable Guard is therefore looped into the cable to be monitored via these two connections.

NOTE

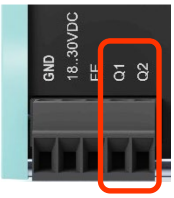
The cable measurement is carried out at the lower "Guard DATA" connection over the entire cable (minimum length 2 m) up to the connected communication partner. The Cable Guard does not change the content of the data transmission between the DATA connections.

5.3 Connecting the data connection (LAN)

The "LAN" data connection enables access to the web server of the monitoring electronics via a TCP/IP network. The website displays the status of the cable to be monitored and allows the Cable Guard to be configured. Furthermore, the status of the cable to be monitored can also be sent to databases or a cloud via MQTT.

Further information on accessing the website and configuration can be found in chapter 7. The use of the MQTT Publisher is explained in chapter 7.3.3.

5.4 Connecting the digital outputs (Q1/Q2)



The digital outputs Q1 and Q2 are only active after the teach-in has been completed.

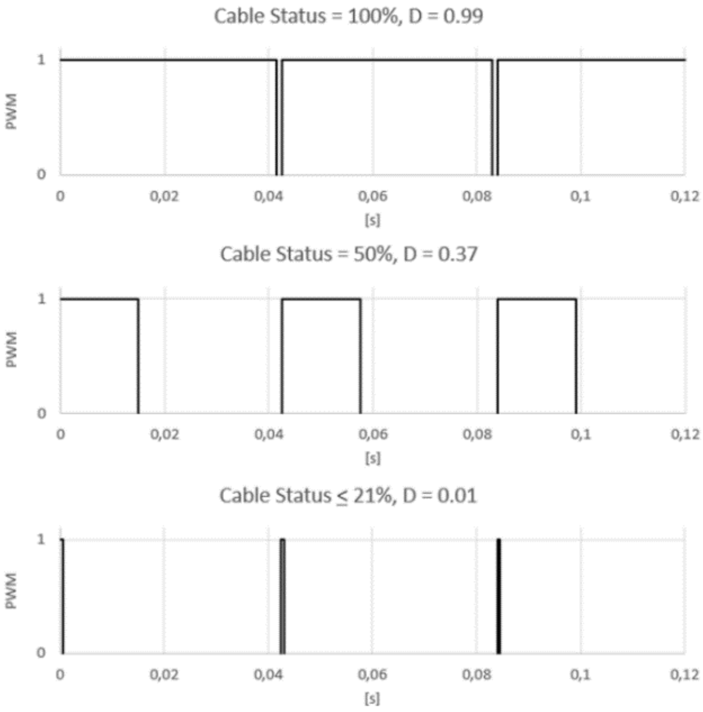
The digital output Q1 can signal that maintenance is required for the cable if the value falls below a configurable threshold ("Alarm threshold for Q1"). The default value is 80%. The output switches to HIGH (NO contact function) when the value falls below this level.

If data communication is interrupted at the "Guard" connection, the Q1 output also switches to HIGH. Further information on configuring the threshold value can be found in chapter 7.1.

The digital output Q2 emits a pulse width modulated signal, which is directly assigned to the "Cable Status" in its duty cycle D. The basic frequency is 24 Hz, the duty cycle varies from 99% (Cable Status = 100%) to 1% (Cable Status < 21%). If data communication is interrupted at the "Guard" connection, a duty cycle of D = 1% is output.

With a measured duty cycle of D %, the cable status is as follows (in %):

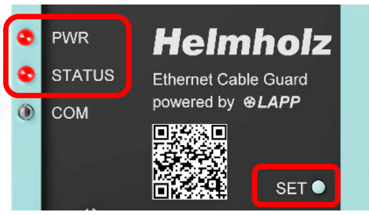
$$\mathit{Cable\ Status}\,[\%] = \frac{D\,[\%]}{1.24} + 20$$



6 Initial Startup ("Teach-In")

Please connect the device to the power supply. Please also note the information above on using the functional earth (FE).

As soon as the DATA connections are connected via Ethernet cables and the links are in operation (see ports of the RJ45 connections), a Teach-In must be carried out for the device to function correctly (this also applies to any cable replacement).

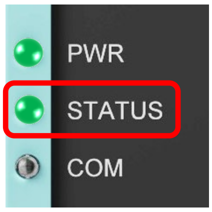


To do this, press the SET button for 20 seconds. As soon as the PWR and STATUS LEDs light up red continuously, the Teach-In is started.
Now release the SET button. The PWR LED now lights up green and the status LED flashes green, the Teach-In is carried out and the cable is now calibrated.

Once the Teach-In process is complete, the PWR and STATUS LEDs light up green continuously. This is the normal operating status of the device. Monitoring of the cable is now active.

The Teach-In values are permanently stored in the device and are retained even in the event of a power failure or a firmware update (software update).

The Teach-In procedure is only necessary after a new installation of the Cable Guard or after replacing the cable.



The status of the cable is displayed via the STATUS LED:

Green = The cable is OK

Flashing red = Maintenance of the cable is required (plan replacement)

Permanently red = The cable is defective

WARNING

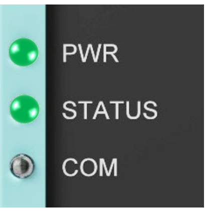
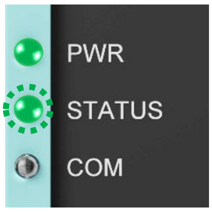
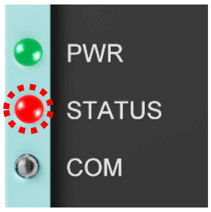
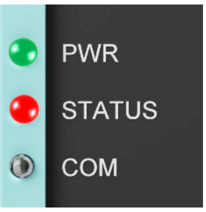
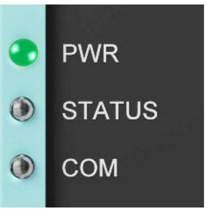
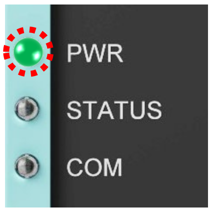
Data transmission between the two DATA connections only works if the Cable Guard is supplied with power and is in normal operating mode!

Further configuration and more information about the status of the Cable Guard can be found on the device's website, see chapter 7.

NOTE

If the Cable Guard is restarted after a Teach-In or if there has been a power failure, the measurement takes a few seconds until a measured value is available again. This is indicated after the restart by a green flashing STATUS LED (initialization).

6.1 Display of the operating statuses via the LEDs

Ready for operation & Line is OK: PWR and STATUS are permanently green  	**Teach-In / Initialization:** PWR is permanent green STATUS flashes green 
Maintenance required: PWR is permanent green STATUS flashed red  	**Cable defective:** PWR is permanent green STATUS is permanent red 
No teach-in performed: Only PWR is green  	**Teach-in faulty:** PWR flashes alternately red/green 

7 Configuration and diagnostics via the web interface

7.1 Access to the website

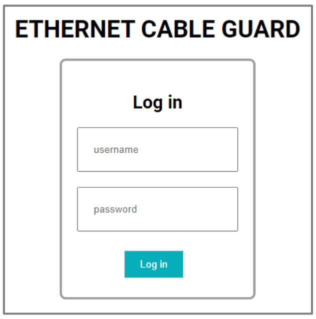
Connect the LAN interface of the Cable Guard to your PC using a standard Ethernet cable. When accessing the website for the first time, set your PC interface to the appropriate subnet, e.g. with the IP address 192.168.0.1 with subnet mask 255.255.255.0 for LAN access.

Open the website in a current browser with "https://192.168.0.32".

NOTE

For security reasons, the web interface can only be accessed via a secure HTTPS connection. To access the website, an exception rule may need to be confirmed in the browser. In the "Settings" menu, you can store your own certificate for connection security if required.

When you log in for the first time, you will be asked to set a password for the default user "admin". The password must be at least 8 characters long.



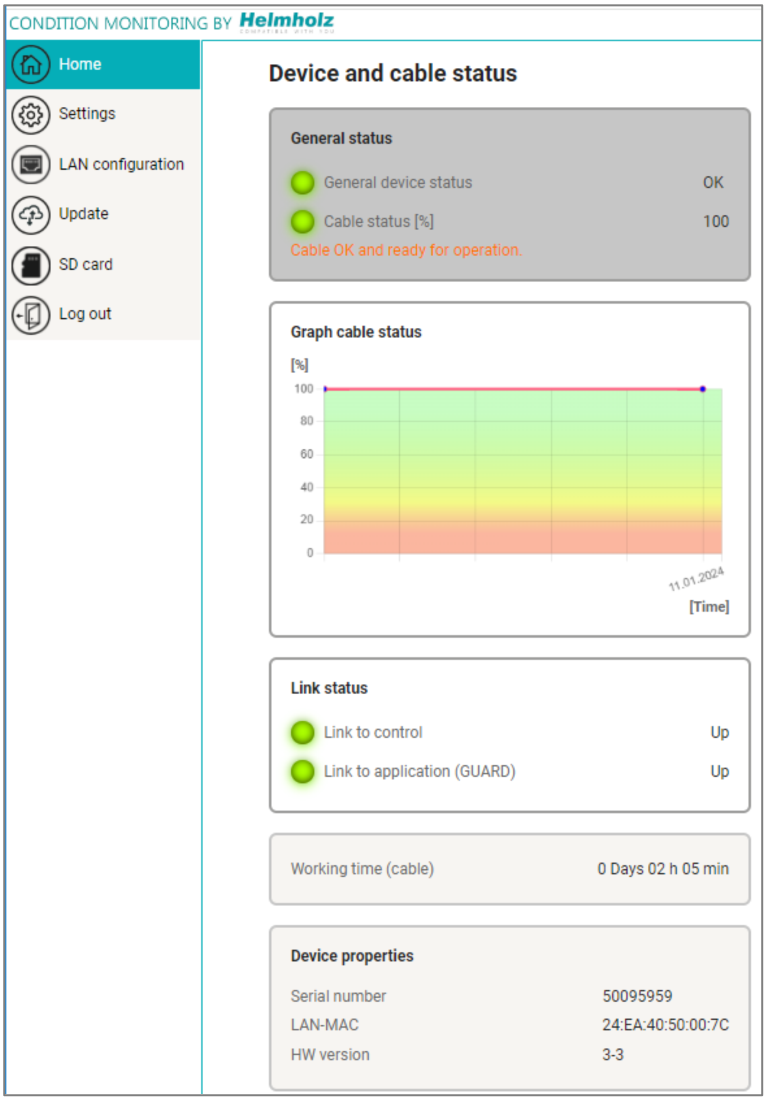
WARNING

Please memorize the password well! For security reasons, there is no way to reset the password without resetting the device to factory settings.

7.2 Main view

After logging in, the Cable Guard "Home" website always opens. The main view contains information about the device and cable status.

The menu on the left-hand side contains additional functions for further configuration or firmware updates.



Device and cable status

General status

● General device status	OK
● Cable status [%]	100

Cable OK and ready for operation.

Graph cable status

Link status

● Link to control	Up
● Link to application (GUARD)	Up

Working time (cable)	0 Days 02 h 05 min

Device properties

Serial number	50095959
LAN-MAC	24:EA:40:50:00:7C
HW version	3-3

7.3 Configuration

7.3.1 Basic configuration "Settings"

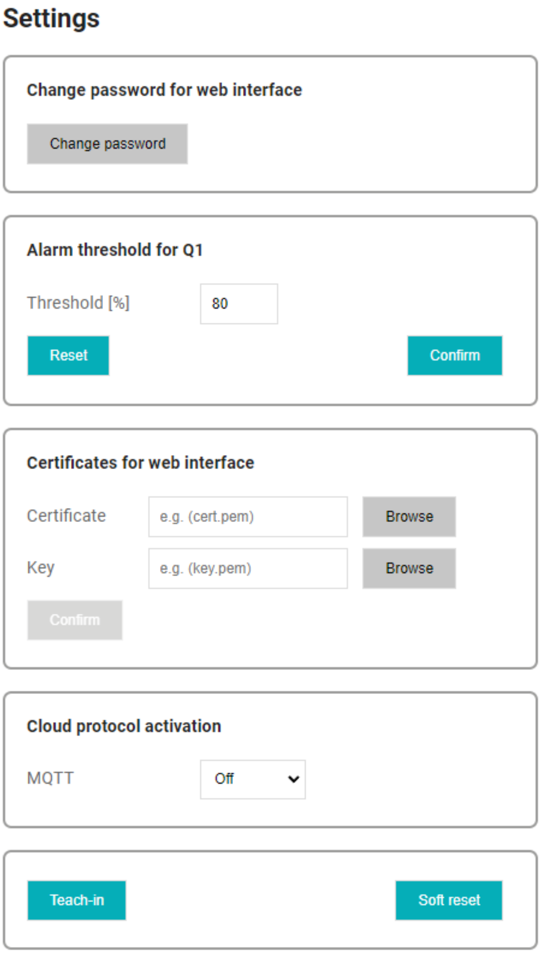
The basic settings can be made in the "**Settings**" menu.

The "**Change password**" button can be used to change the password of the default user "admin".

The "**Alarm threshold for Q1**" can be used to set the limit value for activating output Q1. If the "Cable status" reaches or falls below the value set here, output Q1 is activated permanently.

The Cable Guard website is transmitted to the browser with SSL security. An internal certificate is used for this in the factory settings. This cannot be authenticated by the browser. It is not possible for the browser to confirm the identity of the device. To enable this, a certificate and an associated public key suitable for the network in which it is used can be stored for the Cable Guard.

The MQTT Publisher can be activated under "**Cloud protocol activation**". Further information on this can be found in section 7.3.3.



Settings

Change password for web interface

Alarm threshold for Q1

Threshold [%] 80

Certificates for web interface

Certificate e.g. (cert.pem)

Key e.g. (key.pem)

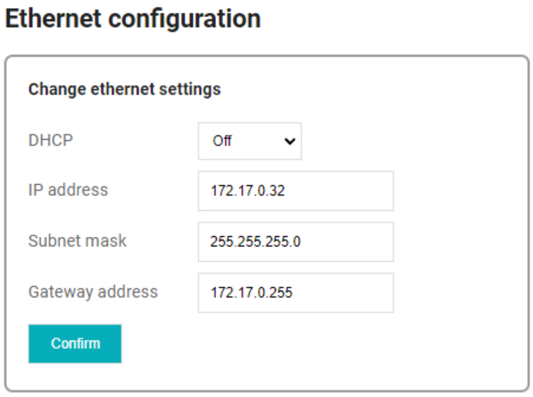
Cloud protocol activation

MQTT Off

7.3.2 Ethernet configuration (LAN)

In the "**Ethernet configuration**" dialog, you can set the LAN IP address, the subnet mask and the gateway to suit your network.

If a DHCP server is available in your network for assigning the IP address, you can set "DHCP: On" so that the Cable Guard is assigned the IP address from this server.



Ethernet configuration

Change ethernet settings

DHCP	Off
IP address	172.17.0.32
Subnet mask	255.255.255.0
Gateway address	172.17.0.255

7.3.3 Sending the cable status via MQTT

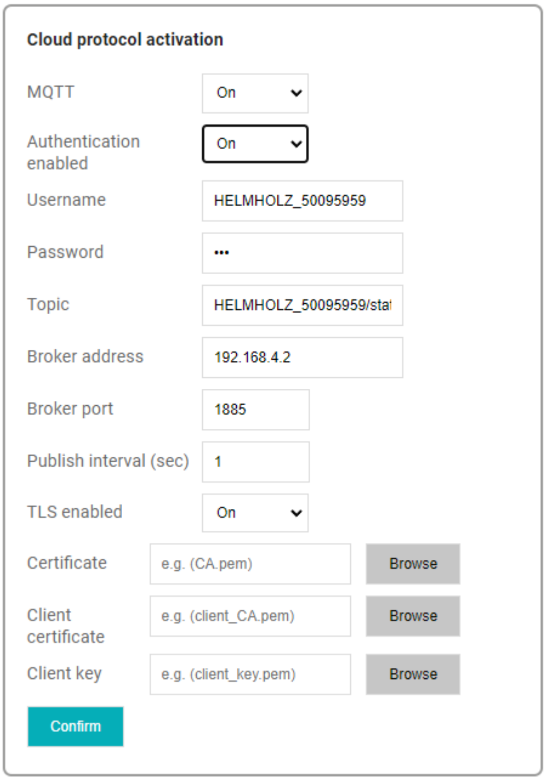
The built-in MQTT Publisher can be activated in the "Settings" menu under "**Cloud protocol activation**". The MQTT Publisher regularly sends the "cable status" as an MQTT message to an MQTT broker, which can be located in the local network or in the cloud.

An MQTT message always consists of a name ("Topic") and the content ("Payload").

The name of the message can be freely selected in the "Topic" input field but should be in a meaningful context. No spaces or special characters are allowed in the topic name.

MQTT messages are always sent to a broker, which then forwards the message to subscribers. The IP address and port of the broker can be specified in "Broker address" and "Broker port".

MQTT also enables TLS (SSL) encryption of the transmission. For this, a certificate for the broker ("Certificate") and the certificate ("Client certificate") and the public key ("Client key") for the client/MQTT publisher must be uploaded.



Cloud protocol activation

MQTT	On	
Authentication enabled	On	
Username	HELMHOLZ_50095959	
Password	•••	
Topic	HELMHOLZ_50095959/stat	
Broker address	192.168.4.2	
Broker port	1885	
Publish interval (sec)	1	
TLS enabled	On	
Certificate	e.g. (CA.pem)	Browse
Client certificate	e.g. (client_CA.pem)	Browse
Client key	e.g. (client_key.pem)	Browse

The structure of the payload sent in the MQTT message is predefined and uses the JSON format:

```
    {
            „CableStatus“:  99,
            „General“:  1,
            „LinkToControl“:  1,
            „LinkToApplication“:  1,
            „Uptime“:  „49680“,
    }
```

“`CableStatus`” displays the cable quality from 0 to 100%; if no teach-in has been performed, this value is 0.

“`General`” corresponds to "General device status" from the web interface (0 = Not OK / 1 = OK).

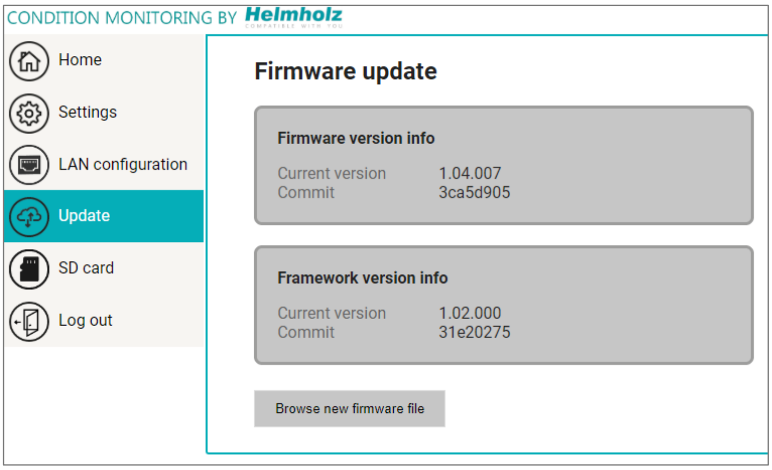
“`LinkToControl`”: Link status of the upper DATA RJ45 (0 = no link / 1 = link present).

“`LinkToApplication`”: Link status of the GUARD DATA RJ45 (0 = no link / 1 = link present).

“`Uptime`”: Measuring time in seconds for the cable measurement; if no Teach-In has been carried out, this value is 0.

7.4 Firmware Update

The firmware update can be accessed on the web interface via the "Update" menu item. The current firmware is displayed here and a new firmware can be uploaded to the device using the "Browse new firmware file" button.



Firmware update

Firmware version info

Current version 1.04.007
Commit 3ca5d905

Framework version info

Current version 1.02.000
Commit 31e20275

The latest firmware can be found on the website in the "Ethernet Cable Guard" product area via the link www.helmholz.de/goto/700-200-LAN01.

The Cable Guard saves the firmware file in its internal memory. After the device is restarted, the firmware is checked. If the content is correct, the firmware is used, otherwise the device is restarted with the old firmware.

ATTENTION

Operation of the Cable Guard is interrupted during the update process. Data transmission between the two DATA connections is interrupted during the update.

Do not switch off the device during the update process! Switching off the power supply can destroy the device.

All settings, the teach-in values and the current measurement of the cable are not changed by the firmware update.

7.5 Factory Reset

The Cable Guard can be reset to factory settings using the "SET" button when the device is switched on.

When the Cable Guard is reset, the complete configuration and all measurement data are irretrievably deleted and IP settings are reset to the factory settings. The firmware remains up to date.

To activate a reset to factory settings, disconnect the Cable Guard from the power supply. Now press and hold the SET button and switch the power supply back on. After 8 seconds, the PWR LED flashes alternately red/green.

Now release the SET button. The factory reset is now performed, and the Cable Guard then restarts.

NOTE

After a factory reset, the cable must be teached in again!

8 FAQ

What is the Ethernet Cable Guard?

Ethernet Cable Guard is a stationary monitoring device that evaluates the current status of a data cable and displays it as a percentage. This is based on data that is determined from the physical properties of the data transmission.

What is the determined "cable status"?

The real-time display of the cable condition makes it possible to identify the wear limit of a cable and plan the optimum replacement time in advance. This is a value determined from several measured variables for the performance status of the cable. This is indicated in 100% to 20%; below 20%, it is no longer possible to draw reliable conclusions about the functionality of the cable.

How does the measurement of the condition of the cable work?

The output of the "cable status" is based on an algorithm - developed by the company LAPP - which collects, converts and continuously evaluates measured values from various physical transmission parameters. The measured values consist, for example, of protocol-related transmission parameters and/or a quality indicator, which can be calculated from statistics of the level values.

The "user data" (data transmission) is neither influenced nor evaluated. If a teach-in is performed, the line is calibrated and limit values are set according to the parameters. If these limit values are violated during operation, correction values are incorporated into the algorithm.

It is important that the algorithm takes historical values into account. This leads to the following consequence: If a line is subjected to such a mechanical load (far above the specifications) that it cannot physically "age", the "prediction" may be delayed. Example: if the data cable is cut with a side cutter, the cable "ages" abruptly; logically, no "prediction" can be made in advance.

What exactly does the "cable status" mean?

The "cable status" is a quality value for the transmission properties of the data cable on the GUARD DATA, including the connectors. The classification of the areas is based on the model of a traffic light: Green area = cable / transmission properties are OK. Yellow area = maintenance/replacement required. Red area = cable defective.

How do customers benefit from using Ethernet Cable Guard?

In highly dynamic, demanding movements with high speeds and strong torsion, it is advantageous and cost-saving if the connection systems are monitored to avoid unforeseen downtimes and thus an impairment of productivity.

The Ethernet Cable Guard determines the status of a data cable and indicates its performance as a percentage. If the performance falls below a certain value, the device sounds an alarm and the cable must be checked or replaced if necessary.

What can the Ethernet Cable Guard do?

The Ethernet Cable Guard determines the current performance of a data cable from various measured variables and displays this as a percentage. The scope of analysis of the Ethernet Cable Guard is deliberately kept reduced and monitors a data cable and indicates its functionality. This enables better planning of maintenance work.

For which industries is the Ethernet Cable Guard suitable?

The Ethernet Cable Guard can be used wherever data cables are used. Especially in moving applications with high speeds and strong torsion. Such applications are often found in (intra-)logistics, the automotive sector and medical technology. In principle, however, it is suitable for a wide range of industries.

Where is the Ethernet Cable Guard used?

The Ethernet Cable Guard is particularly suitable for data cables that are constantly exposed to "stress", such as

- Movements with high speeds and accelerations
- Changing motion sequences
- Rotations with very high axial torsion angles
- Fast cycle times
- small bending radius

The monitored data line is also used in critical processes where a standstill would result in high to extremely high downtime costs or even personal injury.

The Ethernet Cable Guard is suitable

- for use in Ethernet-based automation technology networks.
- for monitoring data cables in dynamic applications.
- for EtherCAT, EtherNET/IP, PROFINET and many other Ethernet-based applications.
- for use in the control cabinet

Which cables can be monitored with the Ethernet Cable Guard?

The Ethernet Cable Guard can be operated with inexpensive, non-specific data cables as well as with high-quality, customer-specific data cables.

In principle, the Ethernet Cable Guard can monitor all data cables of the 100Base-TX transmission standard specified according to IEEE802.3.

Can the Ethernet Cable Guard monitor any type of data cable?

Helmholz recommends the Ethernet Cable Guard primarily for data lines in accordance with the 100BASE-TX transmission standard (with 100 Mbit/s) in accordance with IEEE 802.3, but also for EtherCAT, EtherNET/IP and PROFINET applications.

Can Ethernet Cable Guard be used on multi-axis kinematics / robots?

Yes, please note that the Ethernet Cable Guard is intended for installation in the control cabinet (protection class IP20, not IP67).

Does Ethernet Cable Guard also work across multiple plug-in points?

Yes, the Ethernet Cable Guard can be used with passively linked network components. No active components may be connected in between. Otherwise it is not possible to identify the faulty cable (localization).

Can Ethernet Cable Guard only monitor one data line?

Yes, the Ethernet Cable Guard monitors the route between two active network components (one or more passively linked data cables). There are often only a few data cables in the dynamically moving part of the system.

How can costs be saved with the Ethernet Cable Guard?

The Ethernet Cable Guard enables maintenance cycles to be optimized, resulting in more efficient personnel and resource planning for planned maintenance work. By determining the performance status, the Ethernet Cable Guard contributes to predictive maintenance and increases machine availability with optimized maintenance work.

How high are the cost savings by using the Ethernet Cable Guard?

This depends, for example, on the previous maintenance cycles, the size of the machine fleet, the number of critical plug-in points, the level of expected costs in the event of a production stoppage and much more. It also depends on the respective scenario in which the customer operates, the goods produced, their critical failure forecast and many other factors.

By using predictive maintenance solutions, maintenance operations can be optimized and costs reduced by using fewer personnel resources. In addition, planned downtimes can prevent unforeseen machine failures and thus downtime costs.

Does the Ethernet Cable Guard influence the data transmission?

The Ethernet transmission is not affected in any way. However, the data transmission is delayed by 735 ns at the physical level (delay at 100 Mbit/s) due to the measuring electronics.

How long can the cable to be monitored be?

The Ethernet Cable Guard supports Ethernet cables up to 100m.

What happens if the Ethernet Cable Guard has no power supply?

Communication via the line to be monitored is interrupted until the power supply is restored.

9 Technical data

Order number	**700-200-LAN01**
Name	Ethernet Cable Guard
Scope of delivery	Ethernet Cable Guard with power supply plug
Dimensions (DxWxH)	35 x 48,5 x 75,5 mm
Weight	Approx. 110 g
LAN interface	
Number / Connection	1
Connection	RJ45
Transmission rate	10/100 Mbps
Protocols	HTTPS Web access; MQTT V3.1.1 & V5
DATA Interfaces	
Number / Connection	2, IN / OUT („Guard“)
Connection	RJ45
Transmission rate	10/100 Mbit/s
Delay	735 ns at 100 Mbps
Outputs (Q1 / Q2)	
Number	2
Type	Q1: Push-Pull (NO) / Q2: Push-Pull (PWM)
Current	Max 0,2 A
Protection	Overload protection, short-circuit protection
Status indication	
Functional status	3 LEDs
Ethernet status	6 LEDs
Power supply	
Voltage supply	24 V DC (18 ... 30 V DC)
Current draw	max. 75 mA at DC 24 V
Power dissipation	max. 1.9 W
Ambient conditions	
Ambient temperature	-40°C ... +65°C
Transport- and storage temperature	-40°C ... +85°C
Relative air humidity	95 % r H without condensation
Protection rating	IP20
Pollution degree	2
Mounting position	As desired
Approvals	CE