



ETHERLINE® GUARD PM03T / PM02TWA

Bedienungsanleitung

Ausgabe 1.1 | 23.11.2022 | ab Firmware V 1.00



Link zur neuesten Version
der Bedienungsanleitung

Hinweise

Alle Rechte, auch die der Übersetzung, des Nachdruckes und der Vervielfältigung dieser Bedienungsanleitung, oder Teilen daraus, vorbehalten.

Kein Teil der Bedienungsanleitung darf ohne schriftliche Genehmigung der U.I. Lapp GmbH in irgendeiner Form (Fotokopie, Fotografie, Mikrofilm oder andere Verfahren), auch nicht für Zwecke der Unterrichtsgestaltung, oder unter Verwendung elektronischer Systeme reproduziert, verarbeitet, vervielfältigt oder verbreitet werden.

Die jeweils aktuelle Version der Bedienungsanleitung finden Sie im Internet unter www.lappkabel.de.

Wir freuen uns über Verbesserungsvorschläge und Anregungen.

Weiter bieten wir Ihnen an, den vollständigen, korrespondierenden Quelltext der jeweiligen Open Source Software gegen einen Unkostenbeitrag von Euro 10,00 als DVD auf Ihre Anfrage hin Ihnen und jedem Dritten zu übersenden. Dieses Angebot gilt für den Zeitraum von drei Jahren, gerechnet ab der Lieferung des Produktes.

Copyright © **U.I. Lapp GmbH** 2022. **Alle Rechte vorbehalten.** Weitergabe sowie Vervielfältigung, Verbreitung und Bearbeitung dieses Dokuments, Verwertung und Mitteilung des Inhaltes sind unzulässig, soweit nicht schriftlich gestattet. Alle Rechte für den Fall der Patenterteilung, Geschmacks- oder Gebrauchsmustereintragung sind vorbehalten.

Änderungen in diesem Dokument:

[illegible]

Inhalt

1	Allgemeines	5
1.1	Sicherheitshinweise	5
1.2	Hinweiszeichen und Signalwörter	5
1.3	Zielgruppe der Bedienungsanleitung	6
1.4	Bestimmungsgemäße Verwendung	6
1.5	Missbrauch	7
1.6	Montage / Demontage	7
1.6.1	Zugangsbeschränkung	7
1.6.2	Einbaulage und Mindestabstände	7
1.6.3	Elektrische Installation	7
1.6.4	Schutz vor elektrostatischen Entladungen	8
1.6.5	EMV-Schutz	8
1.6.6	Betrieb	8
1.6.7	Haftung	8
1.6.8	Haftungsausschluss	8
1.6.9	Gewährleistung	9
1.6.10	Recycling und Entsorgung / WEEE	9
2	Security Empfehlungen	10
3	Übersicht	11
4	Aufbau und Anschluss des ETHERLINE® GUARD	12
4.1	Anschluss der Spannungsversorgung	13
4.2	Anschluss der zu überwachenden Leitung (DATA)	13
4.3	Anschluss der Datenverbindung (LAN / WIFI)	14
4.4	Anschluss der digitalen Ausgänge (Q1/Q2)	14
4.5	Verwendung der microSD-Karte	15
5	Erste Inbetriebnahme („Teach-in“)	16
6	Zugriff auf das Webinterface	19
6.1	Zugriff über LAN	19
6.2	Zugriff über WIFI	19
6.3	Erstanmeldung	20
6.4	Hauptansicht „Home“	21
7	Konfiguration	22
7.1	Grundkonfiguration „Settings“	22
7.2	Ethernet Konfiguration (LAN)	22
7.3	WiFi Konfiguration	23
7.3.1	WiFi Betriebsart umschalten	24
7.3.2	Funktionen der WiFi LED	24

8	Versenden des Kabelzustands per MQTT.....	25
9	Firmwareupdate	26
10	Rückstellen auf Werkseinstellung	27
11	FAQ.....	28
12	Technische Daten.....	31
12.1	ETHERLINE GUARD mit LAN-Verbindung	31
12.2	ETHERLINE GUARD mit WIFI-Verbindung.....	32
12.3	Maßzeichnung.....	33
12.3.1	PM03T	33
12.3.2	PM02TWA	33
13	Anhang A - Einrichten einer MQTT-Verbindung.....	34
13.1	ETHERLINE® GUARD MQTT	34
13.1.1	Standard-MQTT-Thema.....	35
13.1.2	Übermittelte Variablen.....	35
13.1.3	Syntax der veröffentlichten Nachrichten.....	36
13.1.4	Anpassung der MQTT-Einstellungen über das Webinterface - MQTT-Einstellungen.....	36
13.2	Beispiel für eine grundlegende MQTT-Demonstration.....	38
13.2.1	Schritt 1: Einrichtung des ETHERLINE® GUARD als MQTT-Client	38
13.2.2	Schritt 2: Einrichten des Mosquitto-Brokers	40
13.2.2.1	Windows-Installation	40
13.2.2.2	Linux-Installation.....	41
14	Anhang B - SSL und sichere MQTT-Verbindungszertifikate	44
14.1	OpenSSL abrufen	44
14.1.1	Windows	44
14.1.2	Linux.....	44
14.2	Zertifikat und Schlüssel für Webbrowser.....	44
14.2.1	SSL-Zertifikat mit OpenSSL erstellen	45
14.2.2	Installieren von SSL-Zertifikaten	45
14.2.2.1	Einbau auf ETHERLINE® GUARD	45
14.2.2.2	Firefox.....	46
14.2.2.3	Chrome und Edge.....	47
14.3	Zertifikat und Schlüssel für MQTT	48
14.3.1	Erstellen mit OpenSSL	48
14.3.2	Installation von MQTT-Zertifikaten auf dem ETHERLINE® GUARD	50

1 Allgemeines

Diese Betriebsanleitung gilt ausschließlich für Geräte, Baugruppen, Software und Leistungen der U.I. Lapp GmbH.

1.1 Sicherheitshinweise

Die Sicherheitshinweise müssen beachtet werden, um Personen und Lebewesen, materielle Güter und die Umwelt vor Schäden zu bewahren. Die Sicherheitshinweise zeigen mögliche Gefahren auf und geben Hinweise, wie Gefahrensituationen vermieden werden können.

1.2 Hinweiszeichen und Signalwörter



GEFAHR

Wenn der Gefahrenhinweis nicht beachtet wird, besteht die unmittelbare Gefahr für Gesundheit und Leben von Personen durch elektrische Spannung.



WARNUNG

Wenn der Gefahrenhinweis nicht beachtet wird, besteht die wahrscheinliche Gefahr für Gesundheit und Leben von Personen.



VORSICHT

Wenn der Gefahrenhinweis nicht beachtet wird, können Personen verletzt oder geschädigt werden.



ACHTUNG

Macht auf Fehlerquellen aufmerksam, die Geräte oder Umwelt schädigen können.

**HINWEIS**

Gibt einen Hinweis zum besseren Verständnis oder zur Vermeidung von Fehlern.

1.3 Zielgruppe der Bedienungsanleitung

Diese Beschreibung wendet sich ausschließlich an ausgebildetes Fachpersonal der Steuerungs- und Automatisierungstechnik, das mit den geltenden nationalen Normen vertraut ist. Zur Installation, Inbetriebnahme und zum Betrieb der Komponenten ist die Beachtung der Hinweise und Erklärungen dieser Betriebsanleitung unbedingt notwendig.

**WARNUNG**

Projektierungs-, Ausführungs- und Bedienungsfehler können den ordnungsgemäßen Betrieb des ETHERLINE® GUARD beeinträchtigen und Personen-, Sach- oder Umweltschäden zur Folge haben. Es darf nur ausreichend qualifiziertes Fachpersonal die Geräte bedienen!

Das Fachpersonal hat sicherzustellen, dass die Anwendung bzw. der Einsatz der beschriebenen Produkte alle Sicherheitsanforderungen, einschließlich sämtlicher anwendbarer Gesetze, Vorschriften, Bestimmungen und Normen erfüllt.

**HINWEIS**

Die Mindestlänge der zu überwachenden Ethernet Leitung beträgt 2m.

Bitte überprüfen sie vor der Verwendung des Geräts, ob eine neuere Version der Firmware auf der Webseite (nähere Infos zum Firmwareupdate in Kapitel 9) zur Verfügung steht.

1.4 Bestimmungsgemäße Verwendung

Der LAPP ETHERLINE® GUARD dient der Zustandsüberwachung von Ethernet basierten Datenleitungen mit dem Übertragungsstandard 100BASE-TX, mit Fokus auf dynamische Anwendungen.

Die gesamten Komponenten werden mit einer werkseitigen Hard- und Software-Konfiguration ausgeliefert. Die Hard- und Software-Konfiguration passend zu den Anwendungsbedingungen muss durch den Anwender erfolgen. Änderungen der Hard- oder Software-Konfiguration, die über die dokumentierten Möglichkeiten hinausgehen, sind unzulässig und bewirken den Haftungsausschluss der U.I. Lapp GmbH.

**VORSICHT**

Das Gerät darf nicht als alleiniges Mittel zur Abwendung gefährlicher Zustände an Maschinen und Anlagen eingesetzt werden.

Der einwandfreie und sichere Betrieb des Gerätes setzt sachgemäßen Transport, sachgemäße Lagerung, Aufstellung, Montage, Installation, Inbetriebnahme, Bedienung und Instandhaltung voraus.

Die in den technischen Daten angegebenen Umgebungsbedingungen müssen eingehalten werden.

Das Gerät besitzt den Schutzgrad IP 20 und muss zum Schutz vor Umwelteinflüssen in einem elektrischen Betriebsraum oder einem Schaltkasten/Schaltschrank montiert werden. Um unbefugtes Bedienen zu verhindern, müssen die Türen der Schaltkästen/Schaltschränke während des Betriebes geschlossen und ggf. gesichert sein.

1.5 Missbrauch

**WARNUNG**

Die Folgen einer nicht bestimmungsgemäßen Verwendung können Personenschäden des Benutzers oder Dritter, Datenschutzverletzungen sowie Sachschäden an der Steuerung, am Produkt oder Umweltschäden sein. Setzen Sie das Gerät nur bestimmungsgemäß ein!

1.6 Montage / Demontage

1.6.1 Zugangsbeschränkung

Die Baugruppen sind offene Betriebsmittel und dürfen nur in elektrischen Betriebsräumen, Schränken oder Gehäusen installiert werden. Der Zugang zu den elektrischen Betriebsräumen, Schränken oder Gehäusen darf nur über Werkzeug oder Schlüssel möglich sein und nur unterwiesenem oder zugelassenem Personal gestattet werden.

1.6.2 Einbaulage und Mindestabstände

Die Baugruppe ist zur Montage auf eine Hutschiene geeignet, die Einbaulage ist dabei beliebig. Es müssen keine Mindestabstände eingehalten werden, die Zugänglichkeit für Stecker und die SD-Karte muss aber gegeben sein.

1.6.3 Elektrische Installation

Die regional gültigen Sicherheitsbestimmungen sind zu beachten.

1.6.4 Schutz vor elektrostatischen Entladungen

Um Schäden durch elektrostatische Entladungen zu verhindern, sind bei Montage- und Servicearbeiten folgende Sicherheitsmaßnahmen zu befolgen:

- Bauteile und Baugruppen nie direkt auf Kunststoff-Gegenstände (z.B. Styropor, PE-Folie) ablegen und auch deren Nähe meiden.
- ESD-konformes Werkzeug und Kleidung verwenden.
- Bauteile und Baugruppen nicht an Kontakten berühren.

1.6.5 EMV-Schutz

Um die elektromagnetische Verträglichkeit (EMV) in Ihren Schaltschränken und in elektrisch rauer Umgebung sicherzustellen, sind bei der Konstruktion und dem Aufbau die bekannten Regeln des EMV-gerechten Aufbaus zu beachten. Insbesondere ist der Anschluss Funktionserde (FE) mit dem Potentialausgleich zu verbinden.

1.6.6 Betrieb

Betreiben Sie das Gerät nur im technisch einwandfreien Zustand. Die zulässigen Einsatzbedingungen und Leistungsgrenzen müssen eingehalten werden.

Nachrüstungen, Veränderungen oder Umbauten am Gerät sind grundsätzlich verboten.

Das Gerät ist ein Betriebsmittel zum Einsatz in industriellen Anlagen. Während des Betriebs müssen alle Abdeckungen am Gerät und der Installation geschlossen sein, um den Berührungsschutz zu gewährleisten.

1.6.7 Haftung

Der Inhalt dieser Bedienungsanleitung unterliegt technischen Änderungen, die durch die ständige Weiterentwicklung der Produkte der U.I. Lapp GmbH entstehen. Für den Fall, dass diese Bedienungsanleitung technische Fehler oder redaktionelle Fehler enthält, behalten wir uns das Recht vor, Änderungen jederzeit und ohne Ankündigung durchzuführen.

Aus den Angaben, Abbildungen und Beschreibungen in dieser Dokumentation können keine Ansprüche auf Änderung bereits gelieferter Produkte gemacht werden. Über die in der Bedienungsanleitung enthaltenen Anweisungen hinaus sind in jedem Fall die gültigen nationalen und internationalen Normen und Vorschriften zu beachten.

1.6.8 Haftungsausschluss

Die U.I. Lapp GmbH haftet nicht bei Schäden, wenn diese durch nicht bestimmungs- oder sachgemäße Benutzung oder Anwendung der Produkte verursacht wurden.

Die U.I. Lapp GmbH übernimmt keine Haftung für eventuell in der Bedienungsanleitung enthaltene Druckfehler oder sonstige Ungenauigkeiten, es sei denn, es sind gravierende Fehler, die U.I. Lapp GmbH nachweislich bereits bekannt sind.

Über die in der Bedienungsanleitung enthaltenen Anweisungen hinaus sind in jedem Fall die gültigen nationalen und internationalen Normen und Vorschriften zu beachten.

Die U.I. Lapp GmbH haftet nicht bei Schäden, die durch Software, die auf Geräten des Anwenders aktiv ist und über die Fernwartungsverbindung weitere Geräte oder Prozesse beeinträchtigt, schädigt oder infiziert und unerwünschten Datentransfer auslöst oder ermöglicht.

Die U.I. Lapp GmbH haftet nicht bei fehlerhafter Berechnung.

1.6.9 Gewährleistung

Melden Sie Mängel sofort nach Feststellung des Fehlers beim Hersteller an.

Die Gewährleistung erlischt bei:

- Missachtung dieser Betriebsanleitung
- Nicht bestimmungsgemäße Verwendung des Geräts
- Unsachgemäßem Arbeiten an und mit dem Gerät
- Bedienungsfehlern
- Veränderungen am Gerät

Es gelten die bei Vertragsabschluss unter "Allgemeine Geschäftsbedingungen der Firma U.I. Lapp GmbH" getroffenen Vereinbarungen.

1.6.10 Recycling und Entsorgung / WEEE

LAPP beachtet alle gesetzlichen Vorgaben und ist bei den nationalen Registern für Elektroaltgeräte gemäß den Richtlinien registriert.

Die in diesem Dokument beschriebenen Produkte sind schadstoffarm, recyclingfähig und erfüllen die Anforderungen der WEEE-Richtlinie 2012/19/EU zur Entsorgung von Elektro- und Elektronik-Altgeräten.



Die beschriebenen Elektrogeräte sind für den Business-to-Business (B2B) Sektor konzipiert und dem Recycling zuzuführen.

Solche Geräte dürfen gemäß Richtlinie 2012/19/EU über Elektro- und Elektronik-Altgeräte (WEEE) nicht über kommunale Entsorgungsbetriebe entsorgt werden.

Entsorgen Sie die Produkte daher nicht bei öffentlichen Entsorgungsstellen.

Für ein umweltverträgliches Recycling und die Entsorgung Ihres Altgeräts wenden Sie sich an einen zertifizierten Entsorgungsbetrieb für Elektronikschrott oder an Ihren LAPP-Ansprechpartner.

Mehr unter www.lappkabel.de/weee.html

Beachten Sie unterschiedliche länderspezifische Regelungen.

2 Security Empfehlungen

ETHERLINE® GUARD ist eine Netzwerkkomponente und damit ein wichtiges Element in der Betrachtung von Security-Aspekten innerhalb einer Anlage oder eines Netzwerkes. Beachten Sie bei der Verwendung des ETHERLINE® GUARD deshalb folgende Empfehlungen, um nicht autorisierte Zugriffe auf Anlagen und Systeme zu unterbinden.

Allgemein:

- Stellen Sie in regelmäßigen Abständen sicher, dass alle relevanten Komponenten diese Empfehlungen und ggf. weitere interne Sicherheits-Richtlinien erfüllen.
- Bewerten Sie Ihre Anlage ganzheitlich im Hinblick auf die Sicherheit. Nutzen Sie ein Zellen-schutzkonzept („Defense-in-Depth“) mit entsprechenden Produkten.
- Informieren Sie sich regelmäßig über Security Bedrohungen für alle ihre Komponenten

Physischer Zugang:

- Beschränken Sie den physischen Zugang zu sicherheitsrelevanten Komponenten auf qualifiziertes Personal.

Sicherheit der Software:

- Halten Sie die Firmware, sowie alle Kommunikationskomponenten jederzeit aktuell.
- Informieren Sie sich regelmäßig über Firmware Updates für das Produkt.
- Aktivieren Sie nur Protokolle und Funktionen, die Sie wirklich benötigen.
- Schalten Sie Zugriffe, die für den Betrieb nicht benötigt werden, nach der Konfiguration aus
- Deaktivieren Sie Zugriffsmöglichkeiten nach der Konfiguration, die für den Dauerbetrieb nicht benötigt werden.
- Verwenden Sie nach Möglichkeit stets diejenigen Varianten von Protokollen, die mehr Sicherheit bieten.

Passwörter:

- Definieren Sie Regeln und Rollen für die Nutzung der Geräte und die Vergabe von Passwörtern.
- Ändern Sie Standard-Passwörter.
- Verwenden Sie ausschließlich Passwörter mit hoher Passwortstärke.
- Stellen Sie sicher, dass alle Passwörter unzugänglich für unbefugtes Personal sind.
- Verwenden Sie dasselbe Passwort nicht für verschiedene Benutzer und Systeme.

Weitere Informationen zur Thema Security erhalten Sie z.B. hier:

- [Bundesamt für Sicherheit in der Informationstechnik \(BSI\)](#)
- [CERT@VDE](#)
- [Sichere-industrie.de](#)
- [Allianz für Cyber-Sicherheit](#)

3 Übersicht

Der ETHERLINE® GUARD kann zur Überwachung von Ethernet basierten Datenleitungen mit einer Übertragungsgeschwindigkeit von 100Mbit/s (100Base-TX) verwendet werden. Der ETHERLINE® GUARD wird in den Kabelstrang eingeschleift und kann über eine getrennte Netzwerkverbindung (LAN oder WiFi) oder über einen digitalen Ausgang über die Qualität der Kabelverbindung informieren.



Nutzen:

- Erhöhung der Anlagenverfügbarkeit durch planbare Stillstandszeiten → Reduzierung der Instandhaltungskosten
- Einfache Inbetriebnahme mit automatisierter Parametrisierung ("Teach-In" in wenigen Sekunden)
- Erfordert keine neue Datenleitung oder Änderungen am Kabeldesign; Retrofit in die bestehende Netzstruktur ist jederzeit möglich
- Verlässliche IIoT-Kommunikation dank MQTT-Schnittstelle

Anwendungsgebiete:

- Zur Überwachung der Lebensdauer einer ausfallgefährdeten Datenleitung (z.B. funktionskritische Datenleitung in dynamischen oder mechanisch belasteten Anwendungen)
- Geeignet für Datenleitungen gemäß Übertragungsstandard 100BASE-TX (mit 100 Mbit/s) nach IEEE 802.3
- Auch für EtherCAT-, EtherNet/IP- und 2-paarige PROFINET-Anwendungen geeignet
- Zur Verwendung im Schaltschrank (Schutzart IP 20)
- Platzsparend durch einzigartig kompaktes Design
- Zur Verwendung in Ethernet basierten Netzwerken der Automatisierungstechnik

Features:

- Rückmeldung der zu erwartenden Lebensdauer über LED-Anzeige "STATUS", über die Webseite oder per digitalem Ausgang.
- Schwellenwert für Alarmauslösung individuell einstellbar (Lebensdauer 99 - 50%).
- Über MQTT-Schnittstelle in IIoT-Strukturen für Status-/Datenauswertung integrierbar
- WiFi Verbindung als Accesspoint (AP) für mobilen Zugriff oder als Client in einem WLAN-Netzwerk

Ausführungen:

- ETHERLINE® GUARD PM03T, LAN-Verbindung
- ETHERLINE® GUARD PM02TWA, WiFi Verbindung

4 Aufbau und Anschluss des ETHERLINE® GUARD

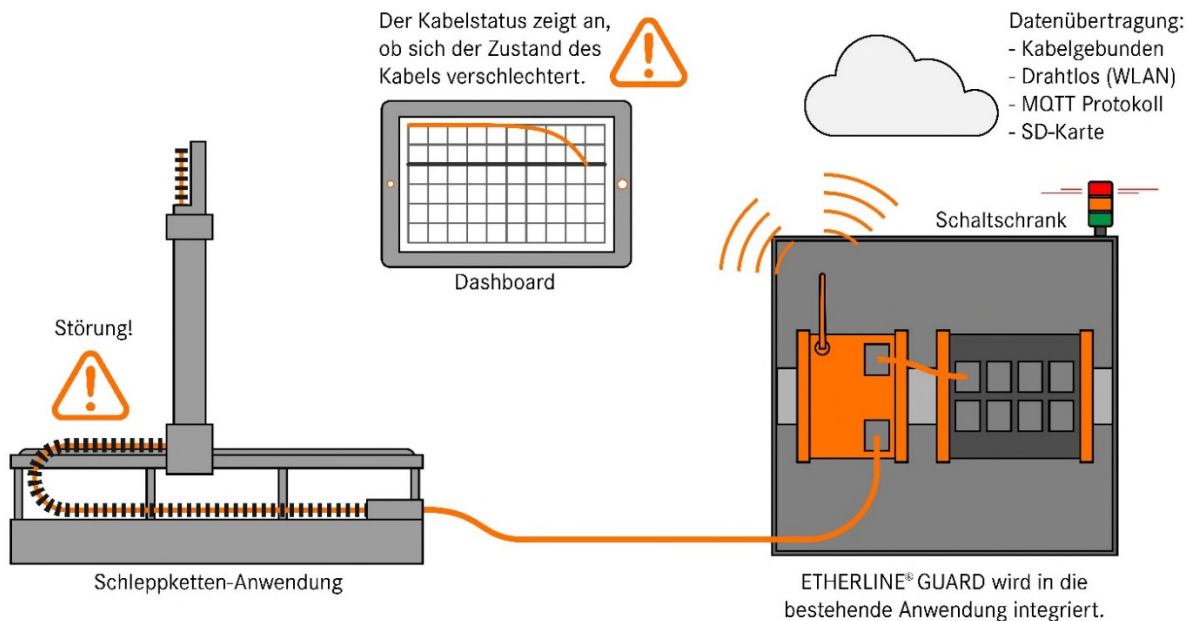
Der ETHERLINE® GUARD hat zwei RJ45-Anschlüsse (DATA) für das zu überwachende Kabel und einen LAN-Anschluss (PM03T) oder einen Antennenanschluss für WiFi (PM02TWA) die Konfiguration über das Webinterface.

Die LEDs am linken Gehäuserand zeigen den Zustand des Gerätes (PWR / STATUS / COM / WIFI) und den Zustand der überwachten Datenleitung an.

Über den Funktionstaster (SET) können verschiedene Funktionen ausgeführt werden.

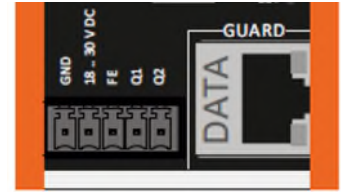


Anwendungsbeispiel:



4.1 Anschluss der Spannungsversorgung

Der ETHERLINE GUARD muss am Weitbereichseingang „18 .. 30 V DC“ und „GND“ über den mitgelieferten Anschlussstecker mit 24 V DC versorgt werden. Der Anschluss „FE“ ist für die Funktionserde. Verbinden Sie diese ordnungsgemäß mit dem Bezugspotential.



HINWEIS

Das Gehäuse des ETHERLINE® GUARD ist nicht geerdet. Bitte verbinden Sie unbedingt den Funktionserdungs-Anschluss („FE“) des Gerätes mit dem Bezugspotential ihres Schaltschranks bzw. Systemaufbaus, um eine korrekte ESD-Ableitung der Antennen- und Netzwerkbusen zu gewährleisten.



ACHTUNG

Wenn das Gerät auf eine Weise verwendet wird, die nicht vom Hersteller angegeben wurde, kann der durch das Gerät gebotene Schutz beeinträchtigt werden. Achten Sie insbesondere auf die korrekte Kontaktierung bei der Kabelmontage. Lesen Sie bei Problemen immer zuerst in der aktuellen Dokumentation nach. Angeschlossene Stromkreise müssen den Anforderungen für Stromkreise mit begrenzter Energie gemäß UL61010-1 entsprechen.

4.2 Anschluss der zu überwachenden Leitung (DATA)

Der ETHERLINE® GUARD hat zwei RJ45-Anschlüsse (DATA) für den zu überwachenden Link, wobei das zu überwachende Kabel am RJ45 Anschluss mit der Kennzeichnung DATA + GUARD angeschlossen sein muss. Der ETHERLINE® GUARD wird über diese beiden Anschlüsse in das zu überwachende Kabel eingeschleift.

Das zu überwachende Kabel (z.B. ein Schleppkabel) muss am unteren Anschluss („Guard“) angeschlossen werden. Der obere DATA Anschluss sollte dann mit dem Kommunikationspartner (z.B. der Steuerung) mit einem weiteren handelsüblichen industrietauglichen Ethernet-Kabel verbunden werden.



HINWEIS

Die Kabelmessung wird am unteren Anschluss „Guard DATA“ über das gesamte Kabel (Mindestlänge 2m) bis zum verbundenen Kommunikationspartner durchgeführt.

Der ETHERLINE® GUARD verändert den Inhalt der Datenübertragung zwischen den DATA-Anschlüssen nicht.



ACHTUNG

Die Datenübertragung zwischen den beiden DATA-Anschlüssen funktioniert nur, wenn der ETHERLINE® GUARD mit Spannung versorgt und im normalen Betriebsmodus ist!

4.3 Anschluss der Datenverbindung (LAN / WIFI)

Die Datenverbindung „LAN“ (PM03T) oder „WIFI“ (PM02TWA) ermöglicht den Zugriff auf den Webserver der Überwachungselektronik per Ethernet Leitung oder per WiFi. Die Webseite zeigt den Zustand des zu überwachenden Kabels an und ermöglicht auch eine Konfiguration des ETHERLINE® GUARDS. Des Weiteren kann der Zustand des zu überwachenden Kabels auch per MQTT an Datenbanken oder in eine Cloud gesendet werden.

Weitere Informationen zum Zugriff auf die Webseite entnehmen Sie dem Kapitel 6.

Die Verwendung des MQTT-Publishers ist im Kapitel 8 erläutert.



ACHTUNG ETHERLINE® GUARD WIFI (PM02TWA)

Das Gerät sollten mit einem Mindestabstand von 20 cm zwischen dem Strahler/Antenne und Ihrem Körper installiert und betrieben werden. Informationen zur Sendeleistung finden Sie in den technischen Daten im Kapitel 12.2.

4.4 Anschluss der digitalen Ausgänge (Q1/Q2)

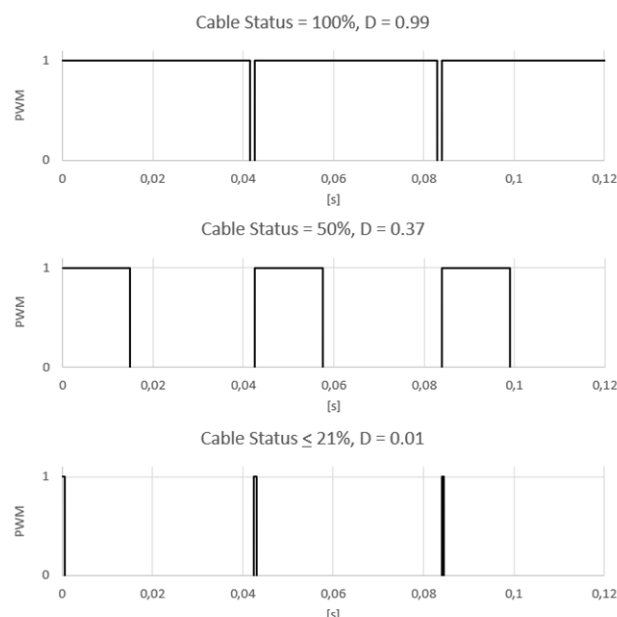
Die digitalen Ausgänge Q1 und Q2 sind erst nach erfolgtem Teach-in aktiv.

Der digitale Ausgang Q1 kann bei Unterschreitung eines konfigurierbaren Schwellwertes („**Alarm threshold for Q1**“) signalisieren, dass eine Wartung für das Kabel notwendig ist. Der Standardwert liegt bei 80%. Der Ausgang schaltet bei Unterschreitung auf HIGH (Schließer-Funktion). Weitere Informationen zur Konfiguration des Schwellwertes finden Sie in Kapitel 7.1. Ist die Datenkommunikation am „Guard“-Anschluss unterbrochen, schaltet der Ausgang Q1 ebenfalls auf HIGH.

Der digitale Ausgang Q2 gibt ein Pulsweiten-moduliertes Signal aus, welches in seinem Tastgrad D direkt dem „Cable Status“ zugeordnet ist. Die Grundfrequenz ist 24 Hz, der Tastgrad variiert von 99% (Cable Status = 100%) zu 1% (Cable Status < 21%). Ist die Datenkommunikation am „Guard“-Anschluss unterbrochen, wird ein Tastgrad von D = 1% ausgegeben.

Bei einem gemessenen Tastgrad von D % ergibt sich folgender Kabelstatus (in %):

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



4.5 Verwendung der microSD-Karte

In die linke Gehäuseseite kann eine microSD-Karte eingesteckt werden. Diese Karte kann zur Diagnose des Gerätes und der Messung Daten aufzeichnen. Die microSD-Karte ist für den normalen Betrieb des Gerätes nicht notwendig! Die Messaufzeichnungen können vom LAPP Support zur Analyse des Gerätes verwendet werden.

PREDICTIVE MAINTENANCE BY  **LAPP**

 Home
 Settings
 WiFi configuration
 Update
 **SD card**
 Log out

SD card information

Current SD card

Name	SH32G
Type	SDHC/SDXC
Total Space	31154 MB
Free Space	31154 MB

Change log level

Log level On ▼

On
Off

Confirm

Note: Make sure to press button "Eject" before removing SD card physically.

Eject

Befindet sich eine SD-Karte im Gerät, werden die Kabel-Messwerte automatisch dort abgespeichert.

Logging = off: Es werden nur die kabelspezifischen Messwerte auf der Karte gespeichert

Logging = on: Zusätzlich zu den Messwerten werden geräteinterne Daten abgelegt. (empfohlen)

Bei der Verwendung einer SD-Karte empfehlen wir, das Logging zu aktivieren, um im Falle einer Auswertung auf mehr Diagnosedaten zugreifen zu können.

Anforderungen an die SD-Karte:

Filesystem: FAT32

Max. Größe: 32 GByte

5 Erste Inbetriebnahme („Teach-in“)

An die untere DATA Buchse (GUARD) wird die zu überwachende Ethernet-Datenleitung angeschlossen. Die obere DATA Buchse ist für die Verbindung mit dem Kommunikationspartner. Hier kann eine handelsübliche industrietaugliche Ethernet-Datenleitung verwendet werden.

Nachdem die beiden DATA Buchsen über Ethernet Leitungen angeschlossen sind und die Ethernet-Links der Kommunikationsverbindung erkannt wurden (das jeweils andere Kabelende ist ebenfalls angeschlossen), muss zur korrekten Funktion des Gerätes einmalig ein **Teach-in** durchgeführt werden.

Eine korrekte Kommunikationsverbindung zwischen den beiden Kommunikationspartnern kann an den LEDs der DATA RJ45 Buchsen erkannt werden. Leuchtet die grüne LED bei beiden RJ45 Buchsen, so steht die Ethernet-Verbindung. Die blinkende gelbe LED an den RJ45 Buchsen zeigt eine aktive Datenübertragung an.

Beim folgenden Teach-in Vorgang wird jetzt das an DATA GUARD angeschlossene Kabel bis zum Kommunikationspartner eingemessen.

Um den Teach-in Vorgang zu starten drücken Sie bitte die Set-Taste mindestens 20s lang. Sobald die PWR-LED und die STATUS-LED gleichzeitig beide rot leuchten, lassen Sie den SET-Taster wieder los.

 PWR  STATUS  WIFI	nach 20s	Teach-in PWR und STATUS leuchten dauerhaft rot.
---	----------	---

- Alle Messdaten (Kabelzustand, Teach-in-Werte) werden gelöscht.
- Das Teach-in wird durchgeführt.
- Andere Einstellungen (Netzwerk, MQTT, digitale Ausgänge) werden beibehalten.
- WiFi Access Point bleibt entsprechend der Ausgangslage aktiviert/deaktiviert.
- Die LEDs erlöschen nach Loslassen des Set Tasters, die gewählte Funktion wird ausgeführt.

Das Einmessen der Datenleitung wird nun im laufenden Betrieb durchgeführt. Dies wird durch eine grün blinkende STATUS-LED angezeigt. Hierbei kann es zu kurzzeitigen Unterbrechungen der Datenverbindung an den jeweiligen Linkpartnern kommen.

 PWR  STATUS  WIFI		Teach-in / Initialisierung PWR leuchtet dauerhaft grün. STATUS blinkt grün (ca. 2Hz, Dauer ca. 1min.).
---	--	---

- Teach-in oder Initialisierung in Progress.
- Nach erfolgreicher Beendigung Wechsel in Betriebszustand Betriebsbereit.

 PWR  STATUS  WIFI		Fehlerhafter Teach-in PWR blinkt abwechselnd rot/grün (ca. 2Hz, Dauer unbegrenzt, bis ein Werksreset oder Teach-in durchgeführt wird).
---	--	--

- Teach-in konnte nicht ausgeführt werden.
- Verkabelung und ggfs. Erdungskonzept überprüfen.
- Teach-in anschließend erneut durchführen.

● PWR ● STATUS ● WIFI	Kein Teach-in durchgeführt PWR leuchtet dauerhaft grün.
--	---

- Es wurde kein Teach-in durchgeführt.
- Kabelzustand wird weder bestimmt noch ausgegeben.
- Teach-in durchführen.

Ist der Teach-in Vorgang abgeschlossen, sollten die PWR-LED und die STATUS-LED dauerhaft grün leuchten.

● PWR ● STATUS ● WIFI	● PWR ● STATUS ● COM	Betriebsbereit PWR und STATUS leuchten dauerhaft grün. WiFi entsprechend dem Betriebszustand blau, grün oder abwechselnd.
---	--	---

- ETHERLINE GUARD befindet sich im Normalbetrieb.
- Überwachte Leitung i.O.
Kabelzustand > eingestellte Alarmschwelle (Default = 80%)
- Digitale Ausgänge schalten je nach Konfiguration (Q1 = NO „low“, Q2 = PWM)
- WiFi
 - o Blau = Access point aktiv
 - o Grün = Client aktiv
 - o Grün blinkend (1Hz) = Gerät versucht Verbindung zu einem Access point aufzubauen
 - o Blau und grün abwechselnd (alle 3s) = Access point und Client aktiv

Tritt während dem Teach-in Vorgang ein Fehler auf, so blinkt die PWR LED grün/rot.



HINWEIS

Der Teach-in Vorgang muss nach jedem Kabeltausch erneut durchgeführt werden!

Die Teach-in Werte werden im Gerät fest hinterlegt und bleiben auch bei einem Stromausfall oder einem Firmware-Update (Softwareaktualisierung) erhalten.

Der ETHERLINE® GUARD ist nun im Mess- und Überwachungsmodus. Der Zustand des Kabels wird über die STATUS-LED, das Webinterface und durch die beiden Ausgänge Q1 & Q2 angezeigt. Zusätzlich kann der Kabelstatus über MQTT gesendet werden.

Leuchtet oder blinkt die STATUS-LED rot, so hat die Messung ergeben, dass sich die elektrischen Kennwerte des Kabels verschlechtert haben und der Schwellenwert der Überwachung unterschritten wurde. Ein Austausch ist (demnächst) ratsam.

 PWR  STATUS  WIFI		Wartung erforderlich PWR leuchtet dauerhaft grün. STATUS blinkt rot (ca. 1Hz).
---	--	---

- ETHERLINE GUARD befindet sich im Normalbetrieb.
- Wartung der überwachten Leitung notwendig
Eingestellte Alarmschwelle (Default = 80%) > Kabelzustand > 20%
- Digitale Ausgänge schalten je nach Konfiguration (Q1 = „high“, Q2 = PWM)

 PWR  STATUS  WIFI		Leitung defekt PWR leuchtet dauerhaft grün. STATUS leuchtet dauerhaft rot
---	--	--

- ETHERLINE GUARD befindet sich im Normalbetrieb.
- Überwachte Leitung ist defekt: Kabelzustand < 20% oder
- Überwachte Leitung ist nicht verbunden.
- Digitale Ausgänge schalten wie folgt (Q1 = „high“, Q2 = PWM, D = 0,01)



HINWEIS

Wird der ETHERLINE® GUARD nach einem erfolgten Teach-in neu gestartet oder gab es einen Spannungsausfall, so benötigt die Messung einige Sekunden, bis wieder ein Messwert vorliegt. Dies wird nach dem Neustart durch eine grün blinkende STATUS-LED angezeigt (Initialisierung).

 PWR  STATUS  WIFI	nach 10s	Soft reset PWR leuchtet dauerhaft grün. STATUS leuchtet dauerhaft rot
---	-----------------	--

- Das Gerät wird neu gestartet, der Datenverkehr wird dazu kurzzeitig unterbrochen.
- Alle Parameter werden beibehalten.
- WiFi Access point bleibt entsprechend der Ausgangslage aktiviert/deaktiviert.
- Die LEDs erlöschen nach Loslassen des Set Tasters, die gewählte Funktion wird ausgeführt.

 PWR  STATUS  WIFI	nach 25s	Abbruch PWR leuchtet dauerhaft grün.
---	-----------------	--

- WiFi Access point, Soft reset und Teach-in werden abgebrochen.
- WiFi Access point bleibt entsprechend der Ausgangslage aktiviert/deaktiviert.
- Die LEDs erlöschen nach Loslassen des Set Tasters, die gewählte Funktion wird ausgeführt.

6 Zugriff auf das Webinterface

Die Webseite zur Anzeige des Kabelstatus und zur Konfiguration des ETHERLINE® GUARD ist über die „LAN“ Schnittstelle (PM03T) oder über WIFI (PM02TW) erreichbar.

Die Webseite des ETHERLINE® GUARD hat im Auslieferungszustand und nach Werksrücksetzen eine Default IP-Adresse. Diese ist auf dem rechten Seitenteil des Gerätes aufgedruckt.

Für die ETHERLINE® GUARD Ausführung „LAN“ ist es die IP-Adresse **192.168.0.32**.

Für die ETHERLINE® GUARD Ausführung „WIFI“ ist es die IP-Adresse **192.168.4.1**.



HINWEIS

Zur optimalen Verwendung und Darstellung empfiehlt Lapp die Nutzung von Google Chrome als Browser.

6.1 Zugriff über LAN

Verbinden Sie die LAN-Schnittstelle des ETHERLINE® GUARD über ein Standard Ethernet Kabel mit Ihrem PC. Die LAN-Schnittstelle unterstützt 10 und 100 Mbit/s. Stellen Sie beim ersten Aufruf der Webseite Ihre PC-Schnittstelle auf das passende Subnetz ein, z.B. mit der IP-Adresse 192.168.0.1 mit Subnetzmaske 255.255.255.0 für den LAN-Zugriff.

Öffnen Sie die Webseite in einem aktuellen Browser mit <https://192.168.0.32>.



HINWEIS

Das Webinterface ist aus Sicherheitsgründen ausschließlich über eine gesicherte HTTPS-Verbindung zu erreichen. Um die Webseite zu erreichen, muss ggf. eine Ausnahmeregel im Browser bestätigt werden.

Im Menü „Settings“ kann bei Bedarf ein eigenes Zertifikat für die Verbindungssicherung hinterlegt werden. Weitere Informationen zum Umgang und dem Einrichten von Zertifikaten finden Sie auf der Homepage des ETHERLINE® GUARD.

6.2 Zugriff über WIFI

Der ETHERLINE® GUARD mit WiFi aktiviert im Werkszustand einen eigenen Accesspoint (AP) mit dem SSID-Namen „LAPP_xxxxxxx“. Die eindeutige Geräte-SSID ist auf dem rechten Seitenteil des Gerätes ablesbar. Das WiFi-Passwort ist „12345678“.

Sobald Sie die Verbindung mit dem WLAN-Netz des ETHERLINE® GUARD aufgebaut haben, kann das Webinterface im Browser unter <https://192.168.4.1> erreicht werden.

Wenn der ETHERLINE® GUARD in ein vorhandenes WLAN integriert werden soll, so kann er auf Client-Betrieb umgestellt werden. Informationen zur WiFi-Konfiguration finden Sie in Kapitel 7.3.

 PWR  STATUS  WIFI	 PWR  STATUS  COM	nach 3s	WiFi Access point (verfügbar bei PM02TWA) PWR leuchtet dauerhaft rot. WiFi leuchtet entsprechend der Funktion blau.
---	--	---------	--

- De-/Aktivierung des WiFi Access Point je nach Ausgangslage.
- Die LEDs erlöschen nach Loslassen des Set Tasters, die gewählte Funktion wird ausgeführt.

6.3 Erstanmeldung

Bei der Erstanmeldung werden Sie aufgefordert, ein Passwort für den Standarduser „admin“ festzulegen. Das Passwort muss mindestens 8 Zeichen lang sein.



ACHTUNG

Bitte prägen Sie sich das Passwort gut ein! Aus Sicherheitsgründen gibt es keine Möglichkeit, das Passwort zurückzusetzen, ohne das Gerät auf Werkseinstellungen zurückzusetzen.

6.4 Hauptansicht „Home“

Nach dem Login öffnet sich immer die „Home“ Webseite des ETHERLINE® GUARD. Die Hauptansicht enthält Informationen über den Geräte- und Kabel-Status.

Im Menu befinden sich weitere Funktionen zur Konfiguration, Firmware-Update, etc.

Mit dem letzten Menupunkt „Log out“ kann der Zugriff auf das Webinterface wieder gesperrt werden.

Details des Menupunkts „Home“ zeigt den Zustand und Informationen des ETHERLINE® GUARD an.

General device status: Zustand des Gerätes

Cable status [%]: Zustand der überwachten Datenleitung. 100% ist der Ausgangszustand. Geringere Werte zeigen eine Verschlechterung des Kabelzustandes an.

Link status: Verbindungsstatus der Leitung zum Netzwerk/Controller (obere DATA-RJ45, „Link to control“) und Verbindungsstatus der überwachten Leitung hin zur Anwendung (GUARD DATA RJ45, „Link to application“).

Working time (cable): Die kumulierte Zeit, in der die überwachte Datenleitung im Messbetrieb war.

Device properties: Seriennummer, MAC-Adresse und HW-Version des ETHERLINE® GUARD.

PREDICTIVE MAINTENANCE BY  LAPP

 Home
  Settings
  LAN configuration
  Update
  SD card
  Log out

Device and cable status

General status

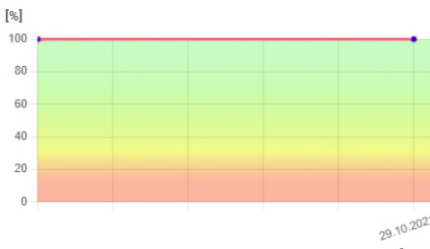


 General device status OK



 Cable status [%] 99

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 05 hh 07 mm

Device properties

Serial number	50080827
LAN-MAC	7C:F9:5C:19:AA:C7
HW version	2-2



HINWEIS

Bitte prüfen Sie auf der Webseite des Produktes unter www.lappkabel.de ob es eine neuere Firmwareversion gibt. Das Firmwareupdate ist in Kapitel 9 beschrieben.

Link zur Firmware: <https://www.lappkabel.de/etherlineguard>



ETHERLINE® GUARD | Ausgabe 1.1 | 23.11.2022

21

7 Konfiguration

7.1 Grundkonfiguration „Settings“

Im Menü „Settings“ können die grundlegenden Einstellungen vorgenommen werden.

Mit dem Button „**Change password**“ kann das Passwort des Standard Benutzers „admin“ geändert werden.

Mit „**Alarm threshold for Q1**“ kann der „cable status“ Grenzwert für die Aktivierung des Ausgangs Q1 festgelegt werden. Erreicht oder unterschreitet der „cable status“ den hier eingestellten Wert, so wird der Ausgang Q1 dauerhaft aktiviert.

Die Webseite des ETHERLINE® GUARD wird SSL abgesichert an den Browser übertragen. Im Werkszustand wird hierfür ein internes Zertifikat verwendet. Dieses kann vom Browser nicht authentifiziert werden, die Bestätigung der Identität des Gerätes ist dem Browser nicht möglich. Um dies zu ermöglichen, kann dem ETHERLINE® GUARD ein Zertifikat („**Certificate**“) und ein zugehöriger öffentlicher Schlüssel („**Key**“) passend für das Netzwerk seines Einsatzes hinterlegt werden.

Unter „**Cloud protocol activation**“ kann der MQTT Publisher aktiviert werden. Weitere Informationen hierzu entnehmen Sie bitte dem Kapitel 8.

Settings

Change password for web interface

Change password

Alarm threshold for Q1

Threshold [%] 90

Reset Confirm

Certificates for web interface

Certificate e.g. (cert.pem) Browse

Key e.g. (key.pem) Browse

Confirm

Cloud protocol activation

MQTT Off

Teach-in Soft reset

7.2 Ethernet Konfiguration (LAN)

Im Dialog „Ethernet Konfiguration“ können Sie die LAN-IP Adresse, die Subnetzmaske und das Gateway passend für ihr Netzwerk einstellen.

Sollte in Ihrem Netzwerk ein DHCP-Server zur Vergabe der IP-Adresse zu Verfügung stehen, so können Sie mit „DHCP: On“ einstellen, dass dem ETHERLINE® GUARD die IP-Adresse von diesem Server zugewiesen wird.

Ethernet configuration

Change ethernet settings

DHCP Off

IP address 192.168.0.32

Subnet mask 255.255.255.0

Gateway address 192.168.0.1

Confirm

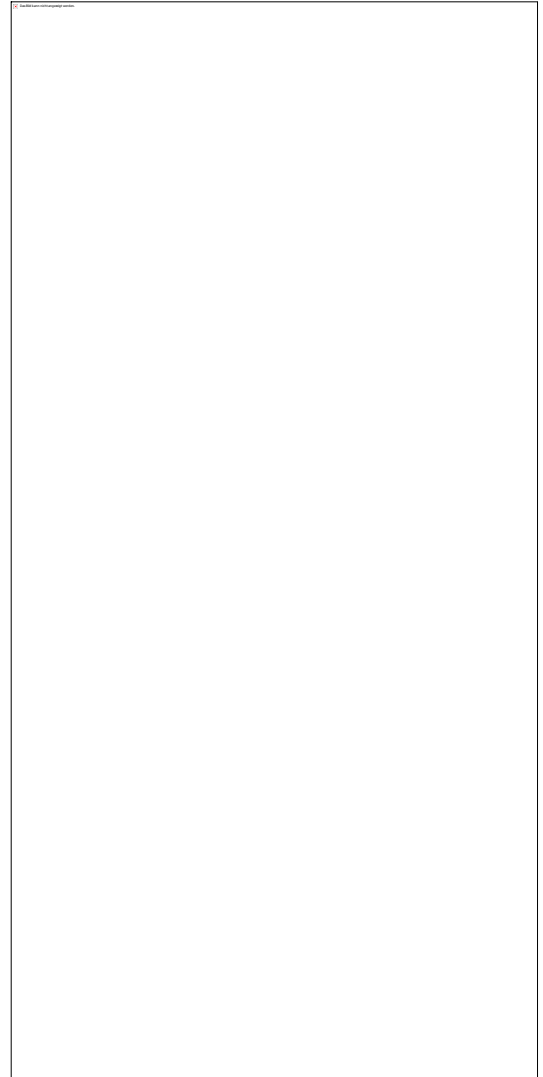
7.3 WiFi Konfiguration

Der ETHERLINE® GUARD arbeitet in Werkseinstellung als Accesspoint (AP). Der erste Zugriff findet somit über den direkten Zugriff z.B. mit einem Handy oder Tablet statt. Der SSID-Name („LAPP_xxxxxxx“) ist auf dem rechten Seitenteil des Gerätes ablesbar. Das Default WiFi-Passwort ist „12345678“.

Sobald Sie die Verbindung mit dem WLAN-Netz des ETHERLINE® GUARD aufgebaut haben, kann das Webinterface im Browser unter <https://192.168.4.1> erreicht werden.

Das Webinterface ist aus Sicherheitsgründen ausschließlich über eine gesicherte HTTPS-Verbindung zu erreichen. Um die Webseite zu erreichen, muss ggf. eine Ausnahmeregel im Browser bestätigt werden.

In der WiFi Konfiguration kann der WiFi Betriebsmodus geändert werden (siehe nächstes Kapitel) und der SSID-Name des Accesspoints angepasst werden.



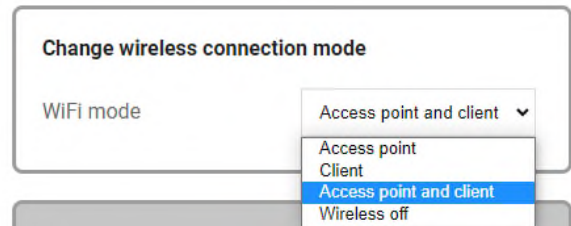
ACHTUNG

Soll der ETHERLINE® GUARD weiterhin als AP erreichbar sein, sollte aus Sicherheitsgründen die SSID und das WLAN-Passwort geändert werden.

7.3.1 WiFi Betriebsart umschalten

Um den ETHERLINE® GUARD auch in ein bestehendes WLAN-Netzwerk einzubinden (Client Betrieb), ändern Sie in der WiFi Konfiguration unter „**Change wireless connection mode**“ den „**WiFi mode**“ entsprechend.

Es kann auf den Client-Betrieb umgeschaltet werden als auch beide Betriebsarten (Accesspoint und Client) aktiv sein. Sind beide Betriebsarten aktiv, so kann der ETHERLINE® GUARD sowohl über einen direkten Zugriff, z.B. von einem Tablet, als auch über den Accesspoint des Firmennetzwerks erreicht werden.

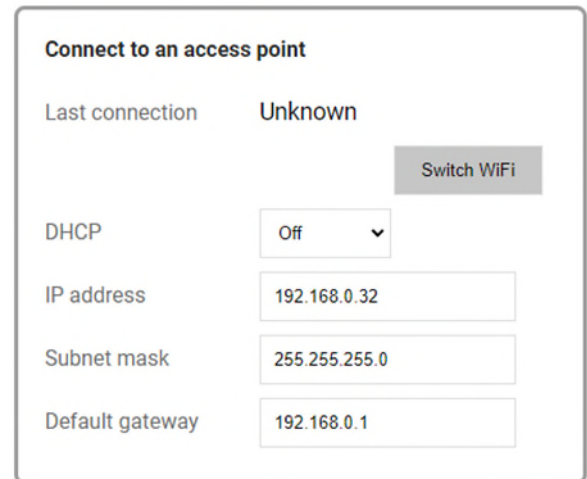


Im Client-Betrieb muss dem ETHERLINE® GUARD noch mitgeteilt werden über welches WiFi-Netzwerk bzw. welchen Accesspoint er sich verbinden soll und welche IP-Einstellungen er in dem WiFi-Netzwerk nutzen soll.

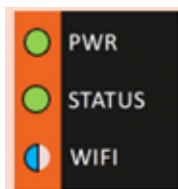
Diese Einstellungen können im Abschnitt „**Connect to an access point**“ vorgenommen werden.

Mit dem Button „**Switch WiFi**“ kann das gewünschte WiFi-Netzwerk ausgewählt werden.

Die Auswahl des WiFi-Netzwerks wird spannungsfest im ETHERLINE® GUARD gespeichert.



7.3.2 Funktionen der WiFi LED



Blau = Accesspoint-Betrieb ist aktiv

Grün = Client-Betrieb ist aktiv

Grün blinkend (1Hz) = Gerät versucht Verbindung zu einem Accesspoint aufzubauen

Blau und Grün abwechselnd (alle 3s) = Accesspoint- und Client-Betrieb aktiv

8 Versenden des Kabelzustands per MQTT

Im Menü „**Settings**“ unter „**Cloud protocol activation**“ kann der eingebaute MQTT Publisher aktiviert werden. Der MQTT Publisher sendet den „cable status“ als MQTT Nachricht regelmäßig an einen MQTT Broker, der sich im lokalen Netzwerk oder in der Cloud befinden kann.

Eine MQTT Nachricht besteht immer aus einem Namen („Topic“) und dem Inhalt („Payload“).

Der Name der Nachricht kann im Eingabefeld „**Topic**“ frei gewählt werden, sollte aber in einem sinnvollen Kontext stehen. Im Topic-Namen sind keine Leerzeichen oder Sonderzeichen erlaubt.

MQTT Nachrichten werden immer an einen Broker gesendet, der die Nachricht dann an Abonnenten („Subscriber“) weiterleitet. Die IP-Adresse und der Port des Brokers kann in „**Broker address**“ und „**Broker port**“ angegeben werden.

MQTT ermöglicht auch eine TLS (SSL) Verschlüsselung der Übertragung. Hierfür müssen dann ein Zertifikat für den Broker („**Certificate**“) und das Zertifikat („**Client certificate**“) und der öffentliche Schlüssel („**Client key**“) für den Client/MQTT Publisher hochgeladen werden.

Der Aufbau der in der MQTT-Nachricht versendeten Payload ist fest vorgegeben und verwendet das JSON-Format:

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

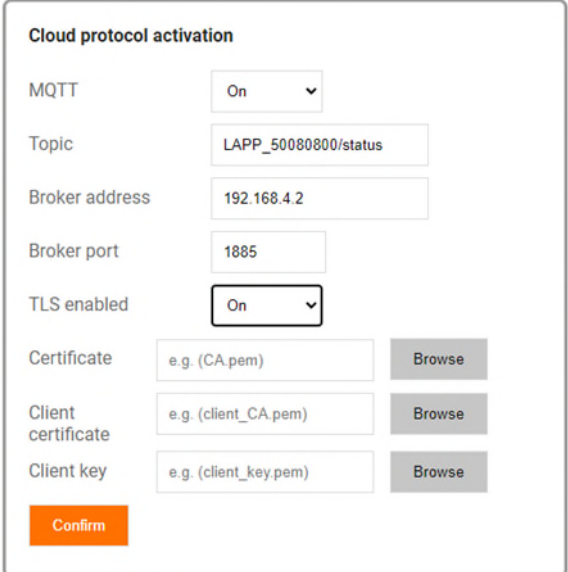
„CableStatus“ zeigt die Kabelqualität von 0 bis 100% an, wurde noch kein Teach-in durchgeführt ist dieser Wert 0.

„General“: Entspricht „General device status“ vom Webinterface (0 = Nicht OK / 1 = OK).

„LinkToControl“: Link-Status der oberen DATA RJ45 (0 = kein Link / 1 = Link vorhanden).

„LinkToApplication“: Link-Status der oberen GUARD DATA RJ45 (0 = kein Link / 1 = Link vorhanden).

„Uptime“: Messzeit in Sekunden für die Kablemessung, wurde noch kein Teach-in durchgeführt ist dieser Wert 0.



9 Firmwareupdate

Die Firmware des ETHERLINE® GUARD kann über das Webinterface sehr einfach aktualisiert werden. Die Firmware erhalten Sie von der LAPP Webseite oder beim LAPP Support.

[Link](#) zur aktuellen Firmware

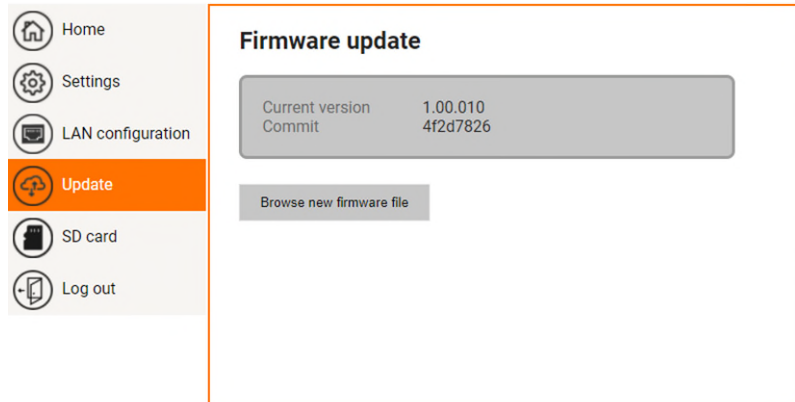
Legen Sie die Firmwaredatei auf Ihrem PC ab.



Auf der Webseite des ETHERLINE® GUARD wählen Sie den Menüpunkt „Update“.

Auf der Firmware update Webseite wird die aktuelle Firmwareversion angezeigt.

Mit „**Browse new firmware file**“ kann die am PC gespeicherte Firmware zum Update ausgewählt werden.



Der ETHERLINE® GUARD speichert die Firmwaredatei in seinem internen Speicher. Nach dem Geräte-Neustart wird die Firmware überprüft. Ist der Inhalt korrekt wird die Firmware verwendet, ansonsten wird das Gerät mit der alten Firmware wieder gestartet.



ACHTUNG

Während des Updatevorganges ist der Betrieb des ETHERLINE® GUARD unterbrochen.

Die Datenübertragung zwischen den beiden DATA Anschlüssen wird beim Update unterbrochen.

Schalten Sie das Gerät während des Updatevorganges nicht aus! Ein Abschalten der Spannungsversorgung kann zur Zerstörung des Gerätes führen.

Alle Einstellungen, die Teach-In Werte und die aktuelle Messung des Kabels werden durch das Firmwareupdate nicht verändert oder beeinflusst.

10 Rückstellen auf Werkseinstellung

Das Rückstellen des ETHERLINE® GUARD auf Werkseinstellung kann mit dem „SET“-Taster beim Einschalten des Gerätes durchgeführt werden.

Es wird beim Rücksetzen des ETHERLINE® GUARD die Konfiguration unwiederbringlich gelöscht und IP- und WiFi-Einstellungen auf den Auslieferungszustand gesetzt. Die Firmware bleibt dabei auf dem aktuellen Stand.

Um ein Rücksetzen auf Werkseinstellung zu aktivieren, trennen Sie den ETHERLINE® GUARD von der Spannungsversorgung. Nun drücken und halten Sie den SET-Taster und schalten die Spannungsversorgung wieder ein. Nach 8 Sekunden blinkt die PWR-LED im Wechsel rot/grün. Lassen Sie den SET-Taster nun los.

Das Werksrücksetzen wird nun durchgeführt und der ETHERLINE® GUARD startet danach neu.

 PWR STATUS WIFI	Gerät vom Strom trennen SET gedrückt halten und dabei Gerät unter Strom setzen nach 8s	Werksreset PWR blinkt abwechselnd rot/grün (ca. 1Hz, Dauer ca. 5s)
--	---	--

- Rücksetzen auf Werkseinstellungen.
- Alle Mess-Daten und Einstellungen werden gelöscht.
- Die LEDs erlöschen nach Loslassen des Set Tasters, die gewählte Funktion wird ausgeführt.
- Nach Beendigung der Funktion Werksreset, automatischer Wechsel in Betriebszustand kein Teach-in durchgeführt.



HINWEIS

Nach einem Werksrücksetzen ist ein erneutes Teach-In des Kabels notwendig, siehe Kapitel 5 - Erste Inbetriebnahme („Teach-in“).

11 FAQ

Was ist ETHERLINE® GUARD?

ETHERLINE® GUARD ist ein stationäres Überwachungsgerät, das den aktuellen Zustand einer Datenleitung auswertet und in Prozent angibt. Grundlage dafür sind Daten, die aus den physikalischen Eigenschaften der Datenübertragung ermittelt werden.

Was genau ist der ermittelte „Kabelzustand“?

Die Echtzeitanzeige des Kabelzustands macht es möglich, die Verschleißgrenze einer Leitung zu erkennen und den optimalen Austauschzeitpunkt im Voraus zu planen. Es handelt sich um einen aus mehreren Messgrößen ermittelten Wert für den Leistungszustand der Leitung. Dieser wird in 100% bis 20% angegeben, unter 20% sind keine verlässlichen Rückschlüsse auf die Funktionsfähigkeit des Kabels mehr möglich.

Wie funktioniert die Messung des Zustands der Leitung?

Die Ausgabe des „cable status“ basiert auf einem Algorithmus, welcher als Rohwerte Messwerte aus diversen physikalischen Übertragungsparametern sammelt, umrechnet und kontinuierlich auswertet. Die Rohwerte bestehen beispielsweise aus protokollnahen Übertragungsparametern und/oder einem Qualitätsindikator, welcher sich aus einer Statistik der Pegelwerte berechnen lässt.

Die „Nutzdaten“ (Datenübertragung) werden dabei weder beeinflusst noch ausgewertet. Wird ein Teach-in durchgeführt, wird die Leitung eingemessen und Grenzwerte entsprechend den Parametern gesetzt. Werden diese Grenzwerte im Laufenden Betrieb verletzt, fließen in den Algorithmus Korrekturwerte ein.

Wichtig dabei ist, dass der Algorithmus historische Werte mit einbezieht. Das führt zu folgender Konsequenz: Wird eine Leitung derart mechanisch belastet (weit über den Spezifikationen), dass diese physikalisch nicht „altern“ kann, erfolgt die „Prediction“ ggfs. zeitverzögert. Beispiel: wird die Datenleitung mit einem Seitenschneider getrennt, „altert“ die Leitung abrupt; es kann logischerweise keine „Prediction“ im Vorfeld erfolgen.

Was sagt der „cable status“ genau aus?

Der „cable status“ ist ein Qualitätswert der Übertragungseigenschaften der Datenleitung am GUARD DATA inklusive der Steckverbinder. Die Einteilung der Bereiche erfolgt nach dem Vorbild einer Verkehrsampel: Grüner Bereich = Leitung / Übertragungseigenschaften sind in Ordnung. Gelber Bereich = Wartung/Austausch erforderlich. Roter Bereich = Leitung defekt.

Wie profitieren Kunden durch den Einsatz von ETHERLINE® GUARD?

Bei hochdynamischen, anspruchsvollen Bewegungen mit hohen Geschwindigkeiten und starker Torsion ist es vorteilhaft und kostensparend, wenn die Verbindungssysteme überwacht werden, um unvorhergesehene Stillstände und somit eine Beeinträchtigung der Produktivität zu vermeiden. ETHERLINE® GUARD ermittelt den Zustand einer Datenleitung und gibt die Leistungsfähigkeit in Prozent an. Sinkt die Leistung unter einen bestimmten Wert, schlägt das Gerät Alarm, und die Leitung muss überprüft oder gegebenenfalls ausgetauscht werden.

Was kann ETHERLINE® GUARD?

ETHERLINE® GUARD ermittelt aus verschiedenen Messgrößen die aktuelle Leistungsfähigkeit einer Datenleitung und gibt diese in Prozent an. Der Analyseumfang von ETHERLINE® GUARD ist bewusst reduziert gehalten und überwacht eine Datenleitung und gibt die Funktionalität dieser an. Damit wird ermöglicht, Wartungsarbeiten besser zu planen.

Für welche Branche eignet sich ETHERLINE® GUARD?

ETHERLINE® GUARD kann überall dort eingesetzt werden, wo Datenleitungen Verwendung finden. Insbesondere bei bewegten Anwendungen mit hohen Geschwindigkeiten und starker Torsion. Solche Applikationen finden sich häufig in der (Intra-)Logistik, dem Automotive-Bereich und der Medizintechnik. Grundsätzlich ist es jedoch für eine Vielzahl an Branchen geeignet.

Wo wird ETHERLINE® GUARD eingesetzt?

ETHERLINE® GUARD eignet sich besonders für Datenkabel, die ständig einer "Belastung" ausgesetzt sind, wie beispielsweise

- Bewegungen mit hohen Geschwindigkeiten und Beschleunigungen
- Wechselnde Bewegungsabläufe
- Rotationen mit axial sehr hohen Verdrehungswinkeln
- schnelle Taktzeiten
- kleine Biegeradien

Die überwachte Datenleitung wird auch in kritischen Prozessen eingesetzt, bei denen im Falle eines Stillstandes hohe bis extrem hohe Ausfallkosten oder sogar Personenschäden entstehen würden.

ETHERLINE® GUARD eignet sich

- für den Einsatz in Ethernet-basierten Netzwerken der Automatisierungstechnik.
- zur Überwachung von Datenleitungen in dynamischen Anwendungen.
- für EtherCAT, EtherNET/IP, PROFINET und vielen weiteren Ethernet basierten Anwendungen.
- für den Einsatz im Schaltschrank

Können auch Kabel von Marktbegleitern überwacht werden? /

Ist ETHERLINE® GUARD auch für Kunden mit Wettbewerbsprodukten interessant?

ETHERLINE® GUARD kann sowohl mit preiswerten, unspezifischen Datenkabeln als auch mit hochwertigen, kundenspezifischen Datenkabeln betrieben werden.

Prinzipiell kann der ETHERLINE® GUARD alle nach IEEE802.3 spezifizierten Datenleitungen des Übertragungsstandard 100Base-TX überwachen. Der Algorithmus zur Bewertung des Kabelzustandes wird allerdings auf LAPP Leitungen getestet und optimiert.

Kann ETHERLINE® GUARD Kabel von Wettbewerbern qualifizieren?

Nein, der ETHERLINE® GUARD kann keine Kabelqualifizierung über die Erfassung standardisierter Messgrößen machen. Er erkennt auch nicht, ob es sich um ein LAPP Kabel oder ein Kabel der Marktbegleiter handelt.

Kann ETHERLINE® GUARD jede Art von Datenleitung überwachen?

LAPP empfiehlt ETHERLINE® GUARD vor allem für Datenleitungen gemäß Übertragungsstandard 100BASE-TX (mit 100 Mbit/s) nach IEEE 802.3, aber auch für EtherCAT-, EtherNET/IP- und PROFINET-Anwendungen, wie zum Beispiel der ETHERLINE® TORSION Cat. 5 oder der ETHERLINE® PN Cat. 5 FD. Diese Leitungen werden häufig in Schleppketten oder torsionsbehafteten Kabelführungen, wie sie in Roboterarmen vorkommen, eingesetzt.

Kann ETHERLINE® GUARD an einer Mehrachskinematik / Roboter verwendet werden?

Ja, es ist zu beachten, dass der ETHERLINE® GUARD für den Einbau im Schaltschrank vorgesehen ist (Schutzklasse IP20, nicht IP67).

Funktioniert ETHERLINE® GUARD auch über mehrere Steckstellen hinweg?

Ja, der ETHERLINE® GUARD kann bei passiv verketteten Netzwerkwerkkomponenten eingesetzt werden. Es darf keine aktive Komponente zwischengeschaltet sein. Ein Rückschluss auf das fehlerhafte Kabel (Lokalisierung) ist nicht möglich.

Kann ETHERLINE® GUARD nur eine Datenleitung überwachen?

Ja, ETHERLINE® GUARD überwacht die Strecke zwischen zwei aktiven Netzwerkkomponenten (eine oder mehrere passiv verkettete Datenleitungen). Häufig liegen im dynamisch bewegten Anlagenteil nur wenige Datenleitungen vor, z.B. in Dresspacks der Roboter.

Wie können Kosten mit ETHERLINE® GUARD eingespart werden?

ETHERLINE® GUARD ermöglicht die Optimierung von Wartungszyklen, damit einhergehend eine effizientere Personal- und Ressourcenplanung bei den geplanten Wartungsarbeiten. Durch die Ermittlung des Leistungszustands leistet ETHERLINE® GUARD einen Beitrag zur Predictive Maintenance und steigert bei optimierten Wartungseinsätzen die Maschinenverfügbarkeit.

Was kostet ETHERLINE® GUARD?

ETHERLINE® GUARD ist im Vergleich zu anderen Monitoringlösungen des Wettbewerbs mit einem niedrigen Einstiegspreis versehen, damit Interessierten eine schnelle und einfache Lösung erhalten, um eine Datenleitung überwachen zu können.

Wie hoch ist die Kosteneinsparung durch Einsatz von ETHERLINE® GUARD?

Das ist abhängig von beispielsweise den bisherigen Wartungszyklen, der Größe des Maschinenparks, der Anzahl der kritischen Steckstellen, sowie der Höhe der erwarteten Kosten bei einem Produktionsstillstand, und vielem mehr. Zudem ist es abhängig vom jeweiligen Szenario, in dem sich der Kunde bewegt, den produzierten Gütern sowie deren kritischer Ausfallprognose und vielen weiteren Faktoren. Durch den Einsatz von Predictive Maintenance-Lösungen lassen sich Wartungseinsätze optimieren und dadurch Kosten durch den geringeren Einsatz von Personalressourcen reduzieren. Zudem lassen sich durch geplante Stillstandzeiten unvorhergesehene Maschinenausfälle und damit Ausfallkosten vermeiden.

Findet eine Beeinflussung der Datenübertragung durch den ETHERLINE GUARD statt?

Die Ethernet-Übertragung wird inhaltlich in keiner Weise beeinflusst. Durch die Messelektronik wird aber die Datenübertragung auf physikalischer Ebene um 735 ns verzögert (Delay bei 100 Mbit/s).

Wie lang kann die zu überwachende Leitung sein?

Der ETHERLINE® GUARD unterstützt Ethernet-Leitungen bis zu 100m.

Was passiert, wenn der ETHERLINE GUARD keine Spannungsversorgung hat?

Die Kommunikation über die zu überwachende Leitung wird unterbrochen, bis die Spannungsversorgung wieder hergestellt wird.

12 Technische Daten

12.1 ETHERLINE GUARD mit LAN-Verbindung

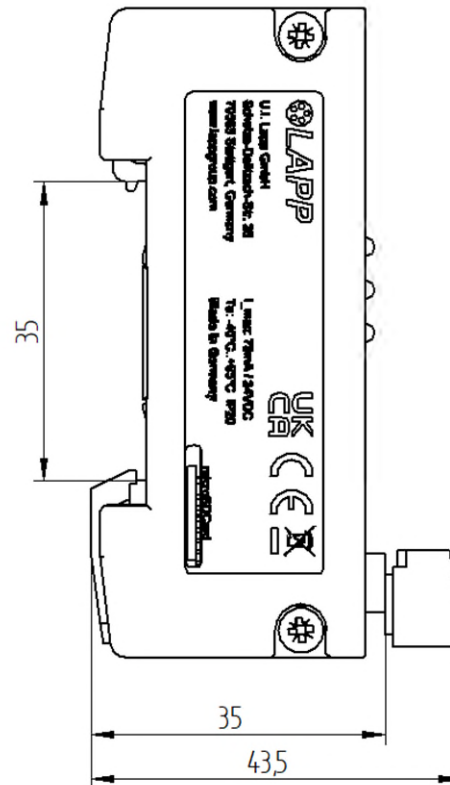
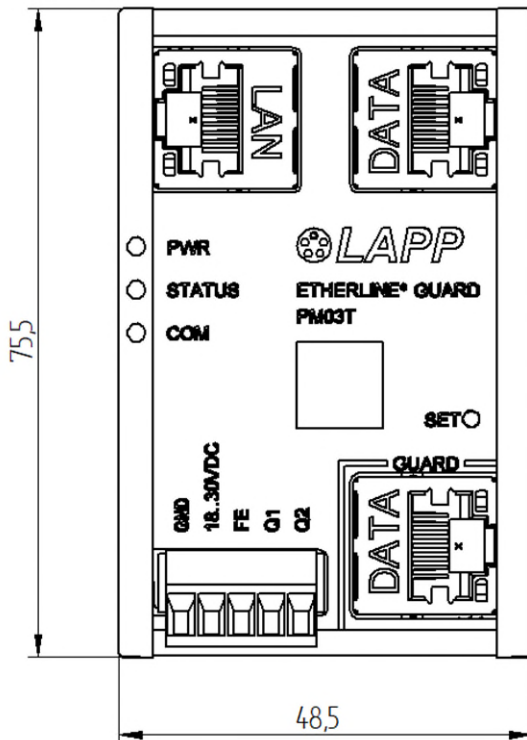
Artikelnummer	21700150
Name	ETHERLINE® GUARD PM03T
Abmessungen (T x B x H)	35 x 48,5 x 75,5 mm (ohne Spannungsversorgungsstecker); 43,5 x 48,5 x 75,5 mm (mit Spannungsversorgungsstecker)
Gewicht	ca. 110 g
LAN-Schnittstelle („LAN“)	
Anzahl	1
Typ	10 Base-T/100 Base-TX
Anschluss	RJ45 Buchse
Übertragungsrate	10/100 Mbit/s
Protokolle	HTTPS, MQTT V3.1.1
Testschnittstellen („DATA“)	
Anzahl	2
Typ	100 Base-TX
Anschluss	RJ45 Buchsen
Übertragungsrate	100 Mbit/s
Delay bei 100 Mbit/s	735 ns
Ausgänge („Q1, Q2“)	
Signalspannung am Ausgang	24 V DC
Anzahl und Art der Ausgänge	2 / max. 0,2 A
PWM Frequenz	24 Hz
PWM duty cycle	0,99 ... 0
Schutz gegen Überlast und Kurzschluss	Ja
Statusanzeige	3 LEDs: Power, Status, COM
Spannungsversorgung	DC 24 V, 18–30 V DC
Stromaufnahme	max. 75 mA bei DC 24 V (ohne Ausgangsleistung von Q1 und Q2)
Verlustleistung	1,92 W
MTBF	10,9 Jahre (gemäß MIL-HDBK-217F)
Einbaulage	Beliebig
Umgebungsbedingungen	
Umgebungstemperatur	-40 °C ... +65°C
Transport- und Lagertemperatur	-40 °C ... +85°C
Relative Luftfeuchte	95 % r. H. ohne Betauung
Verschmutzungsgrad	2
Schutzart	IP20 gemäß EN 60529
Schutzklasse	III gemäß DIN EN 61140
Vibrations- und Stoßfestigkeit	DIN EN 60068-2-6:2008-10 "Vibration"; DIN EN 60068-2-27:2010-02 "Shock"; DIN EN 60068-2-31:2009-04 "Freier Fall"
Zulassungen	CE, UL (in Vorbereitung), FCC (in Vorbereitung)
RoHS, REACH	Ja

12.2 ETHERLINE GUARD mit WIFI-Verbindung

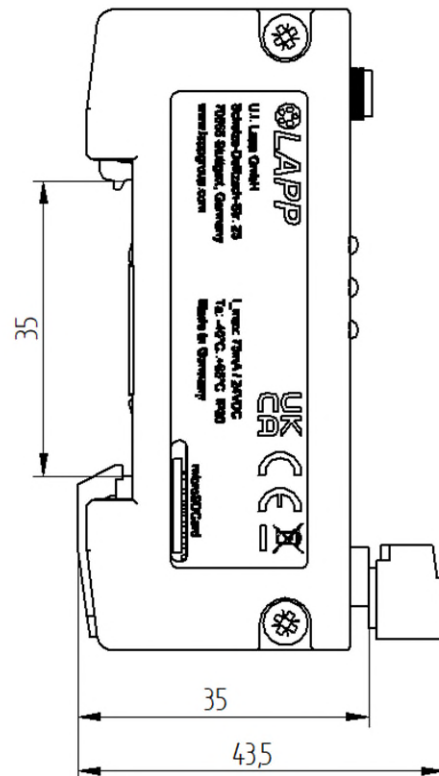
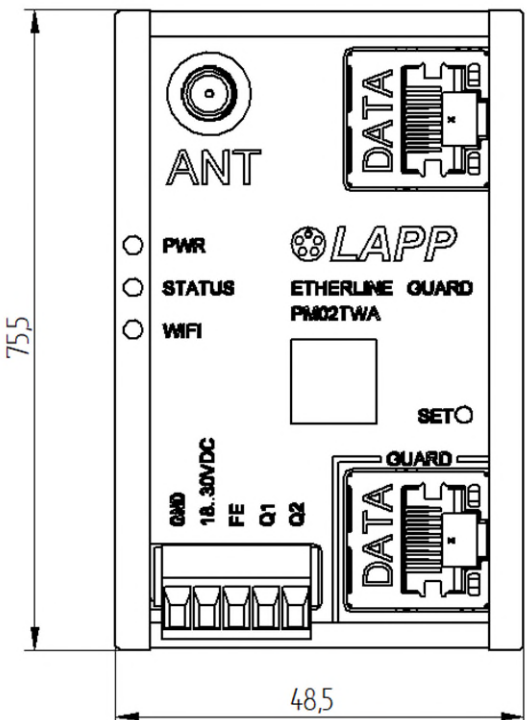
Artikelnummer	21700151
Name	ETHERLINE® GUARD PM02TWA
Abmessungen (T x B x H)	35 x 48,5 x 75,5 mm (ohne Spannungsversorgungsstecker); 43,5 x 48,5 x 75,5 mm (mit Spannungsversorgungsstecker)
Gewicht	ca. 110 g
WLAN-Schnittstelle („WiFi“)	
Anzahl	1
Typ	IEEE802.11b/g/n
Anschluss	SMA Jack, reverse polarity
Empfohlene Antenne	monopole 2,33 dBi
Frequenzbänder	EU (2,412 GHz - 2,472 GHz, Kanäle 1-11)
Sendeleistung	max. 19,22 dBm
Übertragungsrate	802.11b: max. 11 Mbit/s; 802.11g: max. 54 Mbit/s; 802.11n: max. 150 Mbit/s (HT20,MCS0, MCS7)
Betriebsmodi	Access Point, Client
Datensicherheit	WPA 2
Protokolle	HTTPS, MQTT V3.1.1
Testschnittstellen („DATA“)	
Anzahl	2
Typ	100-Base-TX
Anschluss	RJ45 Buchsen
Übertragungsrate	100 Mbit/s
Delay bei 100 Mbit/s	735 ns
Ausgänge („Q1, Q2“)	
Signalspannung am Ausgang	24 V DC
Anzahl und Art der Ausgänge	2 / max. 0,2 A
PWM Frequenz	24 Hz
PWM duty cycle	0,99 ... 0
Schutz gegen Überlast und Kurzschluss	Ja
Statusanzeige	3 LEDs: Power, Status, WIFI“
Spannungsversorgung	DC 24 V (18–30 V DC, SELV und limited energy circuit)
Stromaufnahme	max. 90 mA bei DC 24 V (ohne Ausgangsleistung von Q1 und Q2)
Verlustleistung	2,16 W
MTBF	12,23 Jahre (gemäß MIL-HDBK-217F)
Einbaulage	Beliebig
Umgebungsbedingungen	
Umgebungstemperatur	-40 °C ... +65°C
Transport- und Lagertemperatur	-40 °C ... +85°C
Relative Luftfeuchte	95 % r. H. ohne Betauung
Verschmutzungsgrad	2
Schutzart	IP20 gemäß EN 60529
Schutzklasse	III gemäß DIN EN 61140
Vibrations- und Stoßfestigkeit	DIN EN 60068-2-6:2008-10 "Vibration"; DIN EN 60068-2-27:2010-02 "Shock"; DIN EN 60068-2-31:2009-04 "Freier Fall"
Zulassungen	CE, UL (in Vorbereitung), FCC (in Vorbereitung)
RoHS, REACH	Ja

12.3 Maßzeichnung

12.3.1 PM03T



12.3.2 PM02TWA



13 Anhang A - Einrichten einer MQTT-Verbindung

Der ETHERLINE® GUARD überwacht die Lebensdauer eines ausfallgefährdeten Datenkabels in einem Ethernet-basierten Netzwerk der Automatisierungstechnik und verfügt über eine integrierte MQTT-Funktionalität. Das MQTT-Protokoll kann verwendet werden, um mehrere Geräte mit einer Cloud zu verbinden und verschiedene kritische Anwendungen gleichzeitig zu überwachen. Dieses Kapitel beschreibt die MQTT-Funktionalität und Optionen des ETHERLINE® GUARD in Kapitel 13.1 und zeigt ein einfaches Beispiel-Setup in Kapitel 13.2. Sollten Sie weitere Hilfe oder Anweisungen benötigen, wenden Sie sich bitte an LAPP unter www.lappkabel.com/etherlineguard.

13.1 ETHERLINE® GUARD MQTT

ETHERLINE® GUARD kann verschiedene Statusinformationen einschließlich des "Kabelstatus" zur Überwachung des Kabelverschleißes über die Zeit via MQTT versenden. Diese Informationen stimmen mit denen des Webinterfaces überein. Mit der MQTT-Funktionalität kann die Überwachung verschiedener ETHERLINE® GUARD-Geräte automatisiert werden, so dass ein Alarm ausgelöst wird, sobald ein Kabel das nahe Ende seiner Lebensdauer erreicht hat. Diese Funktionalität ist eine zusätzliche Ausgabeoption zu

- LED "STATUS" zur Anzeige des Kabelstatus
- Digitaler Ausgang Q1, bei dem eine konfigurierbare Alarmschwelle den Ausgang auslöst
- PWM-Ausgang Q2 zur kontinuierlichen Ausgabe des Kabelstatus
- Web-Interface zur grafischen Anzeige des Kabelstatus.



Abbildung 1: ETHERLINE® GUARD-Schnittstellen

MQTT ist ein OASIS-Standard-Nachrichtenprotokoll für das Internet der Dinge (IoT). Es ist als extrem leichtgewichtiger Publish/Subscribe-Messaging-Transport konzipiert, der sich ideal für die Verbindung entfernter Geräte mit geringem Code-Fußabdruck und minimaler Netzwerkbandbreite eignet.¹ Im Folgenden wird ein grundlegendes Verständnis der Hauptfunktionalitäten "Connect", "Publish" und "Subscribe" vorausgesetzt.

¹ Siehe <https://mqtt.org/>

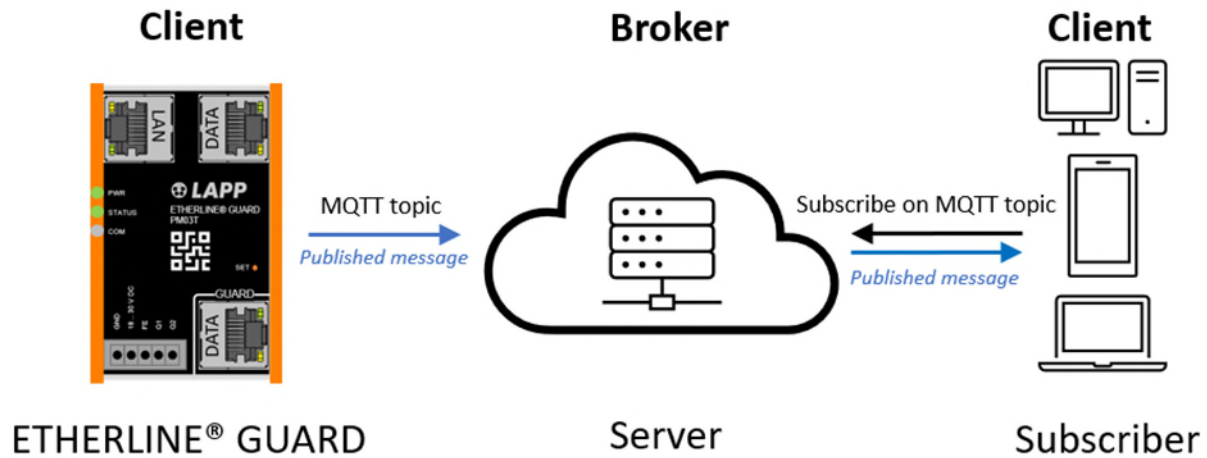


Abbildung 2: Funktionsdarstellung des MQTT-Protokolls²

13.1.1 Standard-MQTT-Thema

Im Umfeld von MQTT bezieht sich das Wort „Topic“ auf einen String, den der Broker verwendet, um Nachrichten für jeden verbundenen Client zu filtern. Für den ETHERLINE® GUARD beginnen die *Standard-MQTT-Topics* mit "LAPP_", gefolgt von der Seriennummer des Gerätes mit einem angehängten "/status":

LAPP_<Serial_Number>/status

Die "<Seriennummer> " wird durch die Seriennummer des Gerätes ersetzt, die auf dem rechten Seitenschild aufgedruckt ist. Dieses *standardmäßige MQTT-Thema* kann geändert werden. Weitere Informationen finden Sie unter **13.1.4**.

13.1.2 Übermittelte Variablen

Innerhalb der ETHERLINE® GUARD Anwendung gibt es einige relevante Variablen, die Teil der versendeten Meldungen sind. Eine Auflistung und Erläuterungen finden Sie im Folgenden.

² <https://mqtt.org/>

Der ETHERLINE® GUARD sendet die folgenden Variablen über das MQTT-Topic /Status-Topic:

Daten	Typ	Mögliche Werte	Erläuterung
"CableStatus"	Integer	Zwischen 100 und 0 (abnehmend)	Zeigt den Kabelstatus des überwachten Datenkabels an.
"General"	Bool als Integer	1: Gut 0: Nicht in Ordnung	Allgemeiner Status des Geräts aus Sicht der Funktionalität
"LinkToControl"	Bool als Integer	1: Verbindung hergestellt 0: Keine Verbindung	Zeigt an, ob ein Kabel am DATA-Port (RJ45) zur Steuerung angeschlossen ist
"LinkToApplication"	Bool als Integer	1: Verbindung hergestellt 0: Keine Verbindung	Zeigt an, ob ein Kabel am GUARD DATA Port zur Anwendung angeschlossen ist
"Uptime"	String	Zeitstempel in Sekunden	Betriebszeit in Sekunden seit dem letzten Teach-in

Tabelle 1: Übertragene Daten mit MQTT

13.1.3 Syntax der veröffentlichten Nachrichten

Die veröffentlichten Nachrichten haben eine vordefinierte Syntax für jedes gesendete MQTT-Topic.

- Syntax des MQTT-Topics "/status":

```
{
    "CableStatus":      100,
    "General":          1,
    "LinkToControl":    0,
    "LinkToApplication": 1,
    "Uptime":           "1234"
}
```

13.1.4 Anpassung der MQTT-Einstellungen über das Webinterface - MQTT-Einstellungen

Die verfügbaren Einstellparameter für eine Übertragung über MQTT finden Sie im Webinterface unter *Menü -> Einstellungen -> Cloud-Aktivierungsprotokoll*:

Cloud protocol activation

MQTT

On ▼

Topic

LAPP_<SN>/status

Broker address

192.168.0.1

Broker port

1885

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

Confirm

Abbildung 3: ETHERLINE® GUARD Webinterface MQTT Einstellungen

- **MQTT:** Die Verwendung des Protokolls kann auf "Ein" und "Aus" gestellt werden.
- **Thema:** String zur Definition des Themas, zu dem die Statusmeldung des Geräts gehört. ("<SN>" steht für "Seriennummer", die durch die Seriennummer des Geräts ersetzt wird. Sie ist auf dem Typenschild der rechten Geräteseite aufgedruckt).
- **Broker-Adresse:** IP-Adresse des MQTT-Brokers.
- **Broker-Anschluss:** Port des Brokers, der auf MQTT-Nachrichten wartet.
- **TLS:** Durch Aktivierung dieser Option wird die MQTT-Kommunikation abgesichert; hier werden Zertifikate importiert, die vom Broker und ETHERLINE® GUARD als Client verwendet werden müssen.

Weitere Informationen finden Sie im Kapitel über das Einrichten einer SSL-Verbindung.

ETHERLINE® GUARD | Ausgabe 1.1 | 23.11.2022

37

13.2 Beispiel für eine grundlegende MQTT-Demonstration

In diesem Kapitel wird ein grundlegendes MQTT-Setup für ETHERLINE® GUARD und ein Beispiel-Setup eines MQTT-Brokers mit der Open-Source-Software Mosquitto vorgestellt.

Anmerkung: Mosquitto ist hier als Beispiel und stellvertretend für mehrere verfügbare MQTT-Broker-Software aufgeführt; es besteht keine zwingende Notwendigkeit, Mosquitto in Kombination mit ETHERLINE® GUARD zu verwenden.

Die beschriebene Vorgehensweise kann als erster Einstieg in MQTT oder zu Demonstrationszwecken verwendet werden. Für einen sicheren Einsatz sollte TLS aktiviert werden, was in diesem Kapitel nicht behandelt wird.

13.2.1 Schritt 1: Einrichtung des ETHERLINE® GUARD als MQTT-Client

Verbinden Sie sich mit dem Web-Interface des ETHERLINE® GUARD (Hinweis: Es spielt keine Rolle, ob das Gerät als Access-Point oder im Client-Modus läuft).

Nachdem Sie sich mit den entsprechenden Anmeldedaten angemeldet haben, gehen Sie bitte auf die Registerkarte Einstellungen (Hinweis: Das Erscheinungsbild kann bei der mobilen Version variieren).

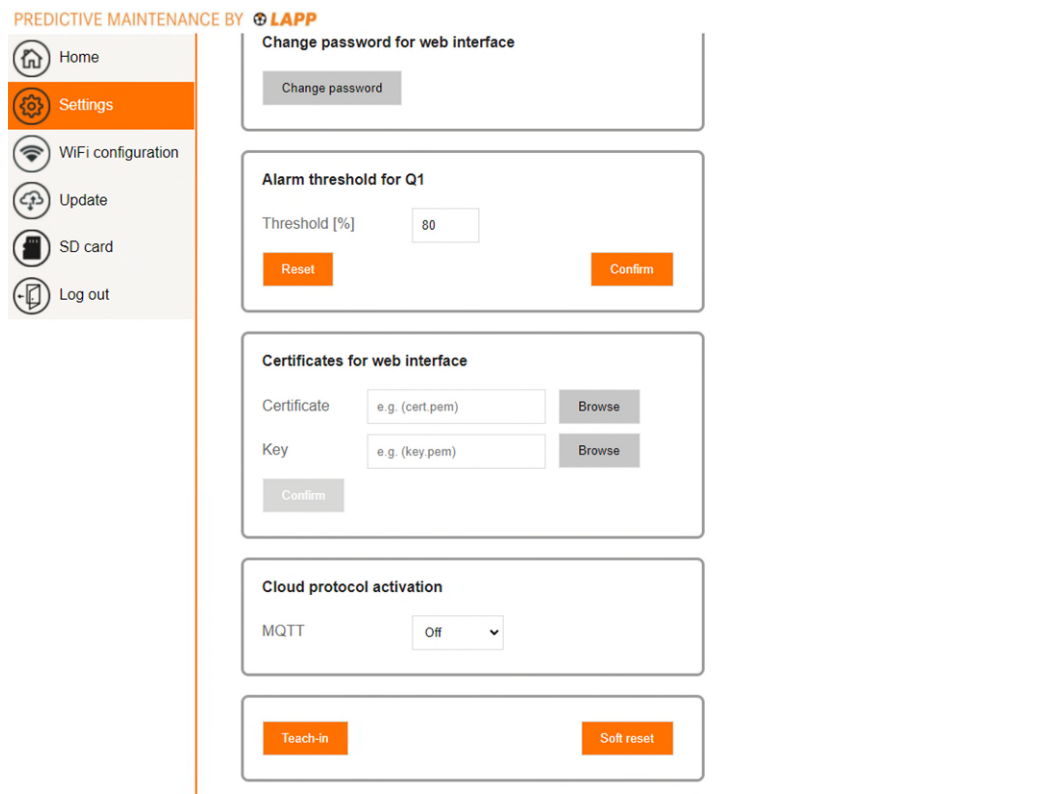
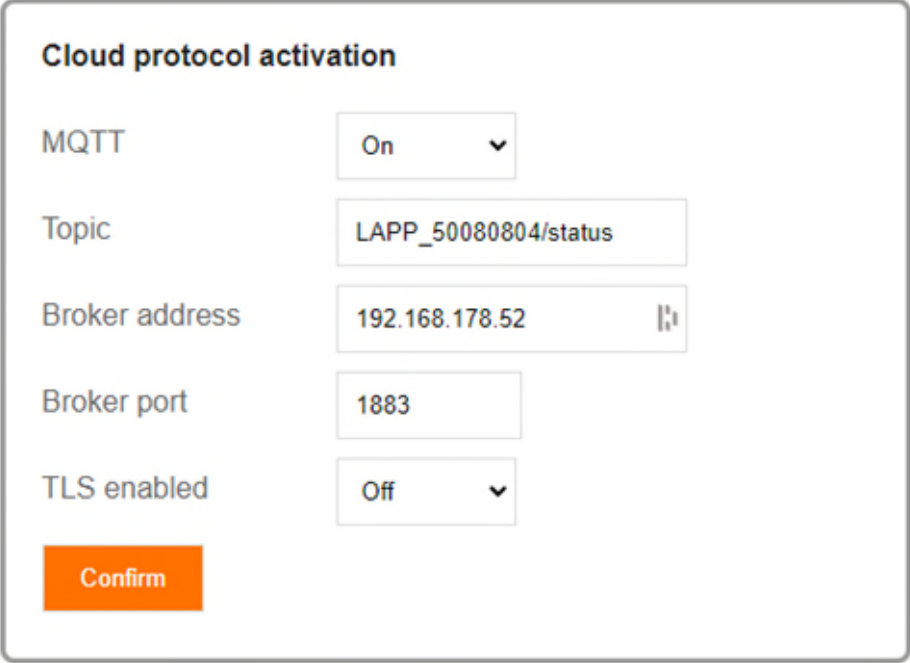


Abbildung 4: ETHERLINE® GUARD Web-Oberfläche → Einstellungen Registerkarte

Scrollen Sie nun nach unten zur Option "Cloud-Protokollaktivierung" und wählen Sie im Dropdown-Menü "Ein". Die folgenden Optionen werden angezeigt:



Cloud protocol activation

MQTT

Topic

Broker address

Broker port

TLS enabled

Confirm

Abbildung 5: ETHERLINE® GUARD Webinterface Option "Cloud Protokoll Aktivierung "

1. Wenn die IP-Adresse des Brokers bereits bekannt ist, kann sie hier eingegeben werden.
 - a. Wenn die IP des Geräts, auf dem der MQTT-Broker installiert werden soll, unbekannt ist, gehen Sie bitte wie folgt vor:

Für Windows:

- i. Öffnen Sie eine Eingabeaufforderung (Windows-Taste und "cmd" eingeben).
- ii. Geben Sie "ipconfig -all" ein.
- iii. Suchen Sie das Netzwerk, mit dem der ETHERLINE® GUARD verbunden ist.
- iv. Blättern Sie nach unten, bis "IPv4" angezeigt wird → . Dies ist die richtige Broker-Adresse.

2. Der Standard-Port für den MQTT-Broker ist 1883 (in einigen Fällen 1885).

Hinweis: Diese Einstellungen können jederzeit geändert werden.

Drücken Sie nun auf "**Bestätigen**". Das ETHERLINE® GUARD-Gerät beginnt nun, MQTT-Nachrichten an den konfigurierten Broker zum konfigurierten Thema zu versenden.

13.2.2 Schritt 2: Einrichten des Mosquitto-Brokers

Mosquitto³ ist eine Open-Source MQTT Software, die sowohl als Broker als auch als Client eingesetzt werden kann. Im Folgenden wird ein einfacher MQTT Broker eingerichtet, der die vom ETHERLINE® GUARD gesendeten Daten beobachtet und empfängt.

13.2.2.1 Windows-Installation

1. Laden Sie die MQTT Mosquitto-Software herunter: <https://mosquitto.org/download/>
2. Der ETHERLINE® GUARD kommuniziert über das Netzwerk, daher muss eine Konfigurationsdatei für den Mosquitto-Broker hinzugefügt werden, um einen Port mit dem folgenden Inhalt zu öffnen:

```
listener 1883
allow_anonymous true
```

Der "Listener" definiert den Port des Brokers, der mit den Einstellungen in der Weboberfläche des Geräts übereinstimmen muss.

Die Option "allow_anonymous" konfiguriert den MQTT Broker so, dass er alle Verbindungen zulässt

Hinweis: Dies ist nur eine Grundeinstellung, bitte verwenden Sie für einen wirklichen Einsatz eine sichere Verbindung mit der TLS-Option.

- a. Um die Konfigurationsdatei zu erstellen, suchen Sie bitte das Mosquitto-Installationsverzeichnis (Standard ist "C:\Programdateien\mosquitto").
- b. Erstellen Sie eine neue Datei in diesem Ordner, z.B. "mosquitto_config.conf" und öffnen Sie sie mit einem Editor.
- c. Fügen Sie nun den Inhalt von oben ein und speichern Sie die Datei

```
listener 1883
allow_anonymous true
```

3. Der Mosquitto-Broker-Server muss neu gestartet werden, bitte gehen Sie wie folgt vor:
 - a. Öffnen Sie ein Eingabeaufforderungs-Fenster (Windows-Taste und "cmd" eingeben)
 - b. Wechseln Sie in das Verzeichnis der Mosquitto-Installation:

```
cd C:\Programdateien\mosquitto
```

- c. Starten Sie den Mosquitto-Broker mit der erstellten Konfigurationsdatei durch Eingabe von:

```
mosquitto.exe -c mosquitto_config.conf -v
```

Die Option "-c [Konfigurationsdatei]" ermöglicht das Laden der von Ihnen erstellten Konfigurationsdatei. Die Option "-v" liefert ausführliche Informationen über die Aktivitäten des Brokers.

Nun wird der Broker gestartet, und in der Eingabeaufforderung sollte folgendes zu sehen sein:

³ Weitere Informationen über die Mosquitto-Software finden Sie unter <https://mosquitto.org/>.

```
mosquitto version 2.0.14 starting
Config loaded from mosquitto.conf.
Opening ipv6 listen socket on port 1883.
Opening ipv4 listen socket on port 1883.
mosquitto version 2.0.14 running
New connection from 192.168.178.39:52467 on port 1883.
New client connected from 192.168.178.39:52467 as LAPP_50080804 (p2, c1, k5, u'LAPP_50080804').
Will message specified (12 bytes) (r0, q1).
status
Sending CONNACK to LAPP_50080804 (0, 0)
Received PUBLISH from LAPP_50080804 (d0, q0, r1, m0, 'LAPP_50080804/status', ... (128 bytes))
Received PUBLISH from LAPP_50080804 (d0, q0, r1, m0, 'LAPP_50080804/status', ... (128 bytes))
```

Abbildung 6: Mosquitto MQTT Broker in der Eingabeaufforderung (Windows)

Die regelmäßig erscheinende Meldung "Received PUBLISH from LAPP_ ..." zeigt an, dass ETHERLINE® GUARD ständig Daten publiziert.

Um die veröffentlichten Nachrichten zu sehen, wird ein zweiter Mosquitto-Client eingerichtet. Er abonniert das MQTT-Topic, für das ETHERLINE® GUARD seine Daten veröffentlicht:

1. Öffnen Sie eine zweite Eingabeaufforderung (Windows-Taste und "Cmd" eingeben)
2. Wechseln Sie mit dem Befehl in das Verzeichnis der Mosquitto-Installation:

```
cd C:\Programdateien\mosquitto
```

3. Starten Sie den Mosquitto-Client, der ein bestimmtes Thema abonniert, indem Sie eingeben:

```
mosquitto_sub.exe -t "+/Status" -h <IP-Adresse> -v
```

Die Option "-t [Thema]" definiert das Thema, für das ein Abonnement erforderlich ist.

Die Syntax "+" vor "/status" weist die Client-Software an, jedes Gerät auszuwählen.

"/status" wählt dann den Sendestatus von diesen Geräten aus. Diese Syntax wird verwendet, wenn die Seriennummer des ETHERLINE® GUARD nicht bekannt ist oder mehrere "/status"-Meldungen von verschiedenen Geräten empfangen werden sollen.

Der Parameter "-h <IP-Adresse>" gibt die die Host-Adresse des Gerätes an, auf der der Broker ausgeführt wird.

Die Option "-v" setzt einen ausführlichen Modus für detailliertere Informationen.

Weitere Informationen zu den MQTT-Abonnementmöglichkeiten finden Sie unter <https://mosquitto.org/man/mqtt-7.html>.

Nun können die Meldungen, die unter dem Thema "/status" veröffentlicht werden, von jedem angeschlossenen ETHERLINE® GUARD gesehen werden. Die Eingabeaufforderung könnte nun wie folgt aussehen:

```
LAPP_50080804/status {
  "CableStatus": 0,
  "General": 1,
  "LinkToControl": 0,
  "LinkToApplication": 1,
  "Uptime": "1797"
}
```

Abbildung 7: Mosquitto MQTT-Client mit Abonnement in der Eingabeaufforderung

Informationen zu den empfangenen Daten finden Sie unter 13.1.2.

13.2.2.2 Linux-Installation

Für eine Installation unter Linux gehen Sie bitte wie folgt vor:

1. Laden Sie die MQTT-Software Mosquitto herunter: <https://mosquitto.org/download/>;
Mosquitto ist ein Debian-eigenes Programm. Es ist auch in Raspbian enthalten, daher ist ein zusätzlicher Download von Mosquitto nicht notwendig.

Stellen Sie sicher, dass Sie die neueste Version verwenden, indem Sie sie aktualisieren

```
sudo apt-get update
```

2. Der Mosquitto-Broker kann nun mit folgendem Befehl gestartet werden

```
mosquitto -p 1885 -v
```

Hinweis: Der Port wird hier definiert, da der Standardwert für die Linux-Installation 1883 ist und möglicherweise bereits ein Broker im Hintergrund läuft. Außerdem müssen die Einstellungen des ETHERLINE® GUARD in der Weboberfläche übereinstimmen.

Fehlersuche: Wenn keine Nachrichten empfangen werden, überprüfen Sie bitte, ob der Port korrekt ist und ob der Port offen ist!

Die Option "- C" kann zur Verwendung der Konfigurationsdatei hinzugefügt werden.

Sobald der Broker gestartet ist, sollte im Terminal folgendes zu sehen sein:

```
mosquitto version 1.5.7 starting
Using default config.
Opening ipv4 listen socket on port 1885.
Opening ipv6 listen socket on port 1885.
New connection from 192.168.178.39 on port 1885.
New client connected from 192.168.178.39 as LAPP_50080804 (cl, k5, u'LAPP_50080804').
Will message specified (12 bytes) (r0, ql).
    status
Sending CONNACK to LAPP_50080804 (0, 0)
Client LAPP_50080804 has exceeded timeout, disconnecting.
Socket error on client LAPP_50080804, disconnecting.
New connection from 192.168.178.39 on port 1885.
New client connected from 192.168.178.39 as LAPP_50080804 (cl, k5, u'LAPP_50080804').
Will message specified (12 bytes) (r0, ql).
    status
Sending CONNACK to LAPP_50080804 (0, 0)
Received PUBLISH from LAPP_50080804 (d0, q0, r1, m0, 'LAPP_50080804/status', ... (123 bytes))
Received PUBLISH from LAPP_50080804 (d0, q0, r1, m0, 'LAPP_50080804/status', ... (123 bytes))
```

Abbildung 8: Mosquitto MQTT Broker im Terminal (Linux)

Um die gesendeten Nachrichten zu sehen, wird das MQTT-Thema in einem neuen Terminalfenster abonniert:

1. Geben Sie folgenden Befehl ein

```
mosquitto_sub -p 1885 -t "+/Status" -v
```

Die Option "-t [Thema]" definiert das Thema, für das ein Abonnement erforderlich ist.

Die Syntax "+" vor "/status" weist die Client-Software an, jedes Gerät auszuwählen.

"/status" wählt dann den gesendeten Status von diesen Geräten aus. Diese Syntax wird verwendet, wenn die Seriennummer des ETHERLINE® GUARD unbekannt ist oder mehrere "/status"-Meldungen von verschiedenen Geräten empfangen werden sollen. Die Option "-v" setzt einen ausführlichen Modus für detailliertere Informationen.

Weitere Informationen zu den MQTT-Abonnementmöglichkeiten finden Sie unter <https://mosquitto.org/man/mqtt-7.html>.

```
LAPP_50080804/status {
  "CableStatus": 0,
  "General": 1,
  "LinkToControl": 0,
  "LinkToApplication": 1,
  "Uptime": "1797"
}
```

Abbildung 9: Mosquitto MQTT Client mit Abonnement im Terminal

14 Anhang B - SSL und sichere MQTT-Verbindungszertifikate

Der ETHERLINE® GUARD verfügt über ein eingebautes Webinterface zur Gerätekonfiguration und MQTT-Funktionalität. Dieses Kapitel behandelt die Installation und Erstellung einer sicheren SSL-Verbindung zum Webinterface und TLS-Zertifikate für eine sichere MQTT-Verbindung. Die Zertifikate für das Webinterface müssen in jedem Webbrowser installiert werden, um eine https-Verbindung zum ETHERLINE® GUARD aufbauen zu können. Zur Erstellung des Zertifikats die in Kapitel 14.2. beschriebenen Schritte notwendig. Um eine sichere MQTT-Verbindung aufzubauen, folgen Sie den Schritten in Kapitel 14.3. Sollten Sie weitere Hilfe oder Anweisungen benötigen, wenden Sie sich bitte an LAPP unter www.lappkabel.com/etherlineguard.

14.1 OpenSSL abrufen

Für eine einfache Möglichkeit, eigene SSL-Zertifikate zu erstellen, können Sie die Open-Source-Software [OpenSSL](https://www.openssl.org/) verwenden.

14.1.1 Windows

Unter Windows ist der einfachste Weg, ein funktionierendes OpenSSL zu bekommen, Git. Wenn Sie bereits Git verwenden, brauchen Sie nur den Git Bash.

Git hier herunterladen <https://git-scm.com/downloads>

Nach der Installation öffnen Sie die Git Bash (drücken Sie die Windows-Taste und geben Sie „Git Bash“ ein).

14.1.2 Linux

OpenSSL ist wahrscheinlich bereits installiert; Sie können dies überprüfen, indem Sie eingeben:

➔ `openssl-version`

Ansonsten installieren Sie OpenSSL mit:

➔ `sudo apt-get install libssl-dev`

14.2 Zertifikat und Schlüssel für Webbrowser

Sie müssen dasselbe Zertifikat und denselben Schlüssel sowohl auf dem Gerät und in Ihrem Browser verwenden.

Zur Erstellung Ihres Zertifikats benötigen Sie eine Konfigurationsdatei. Lapp stellt Ihnen hierfür eine Vorlage „ssl_config.cnf“ zur Verfügung, die Sie an Ihre Erfordernisse anpassen können. Hier ist beispielsweise die IP-Adresse des Etherline Guard definiert, zu dem die verschlüsselte Verbindung aufgebaut werden soll. Sollen verschlüsselte Verbindungen zu mehreren Geräten aufgebaut werden, so ist jede einzelne IP Adresse aufzulisten (siehe Beispiel-Datei).

Es ist wichtig, dass Sie für jedes Zertifikat, das Sie in diesem Kapitel erstellen werden, dieselbe Konfigurationsdatei verwenden.

14.2.1 SSL-Zertifikat mit OpenSSL erstellen

Durch die folgenden Befehle werden die Dateien „server.pem“, „serverkey.pem“ und „server.p12“ erzeugt.

1. Öffnen Sie Git-Bash
2. Wechseln Sie in das Verzeichnis der heruntergeladenen oder selbst erstellten Konfigurationsdatei und geben Sie dann die folgenden Befehle ein, die drei Dateien im selben Verzeichnis erstellen, an dem sich auch Ihre Datei "ssl_config.cnf" befindet:
→ `openssl req -x509 -nodes -days 7300 -newkey rsa:2048 -keyout serverkey.pem -out server.pem -config ssl_config.cnf`

→ `openssl pkcs12 -export -out server.p12 -in server.pem -inkey serverkey.pem -passin pass:lapp -passout pass:lapp`

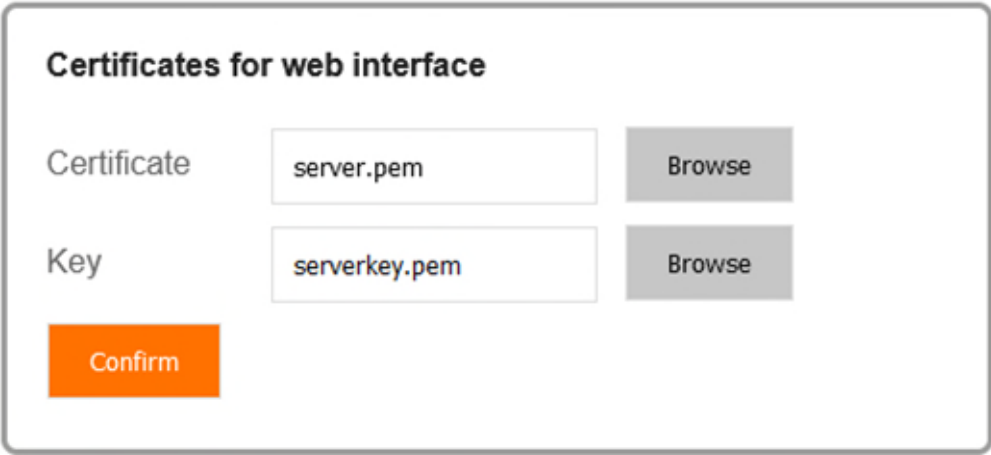
Bitte tragen Sie für das Passwort nach „-passin pass:“ und „-passout pass:“ ihr eigenes sicheres Passwort ein. Das hier verwendete Passwort „lapp“ dient lediglich als Beispiel.

14.2.2 Installieren von SSL-Zertifikaten

Nachdem Sie Ihre Zertifikate und Schlüssel erstellt haben, müssen Sie diese auf dem ETHERLINE® GUARD und in Ihrem bevorzugten Browser installieren (Sie können sie auch auf Ihrem lokalen Zertifikatsserver installieren).

14.2.2.1 Einbau auf ETHERLINE® GUARD

Um die Zertifikate auf dem ETHERLINE® GUARD zu installieren, öffnen Sie das Webinterface und navigieren Sie zum Reiter "Einstellungen". Klicken Sie unter "Zertifikate für Webinterface" auf „Durchsuchen“ und wählen Sie die Dateien wie in Abbildung 10. Klicken Sie dann auf „Bestätigen“. Der Webserver wird neu gestartet.



Certificates for web interface		
Certificate	server.pem	Browse
Key	serverkey.pem	Browse
Confirm		

Abbildung 10: Zertifikatsauswahl ETHERLINE® GUARD

14.2.2.2 Firefox

1. Drücken Sie Win+R und geben Sie "certmgr.msc" ein, es öffnet sich folgendes Fenster. Dies ist der Zertifizierungsmanager, der alle Ihre digitalen Zertifikate auflistet:

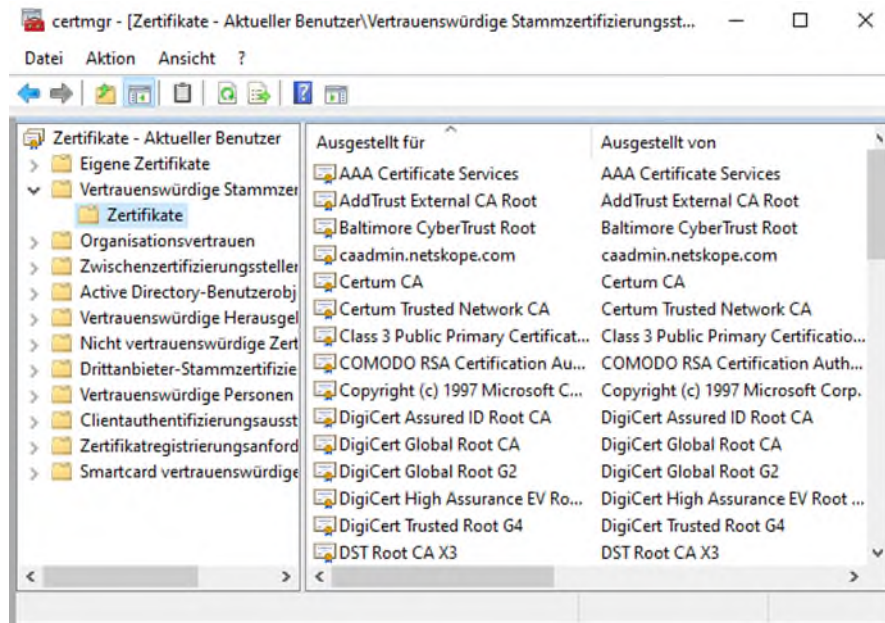


Abbildung 11: Windows-Zertifizierungsmanager

2. Klicken Sie auf „Vertrauenswürdige Stammzertifizierungsstellen“ und mit der rechten Maustaste auf Zertifikate, um ein Kontextmenü zu öffnen.
3. Wählen Sie im Kontextmenü „Alle Aufgaben“ -> „Importieren“, um das unten abgebildete Fenster zu öffnen.
4. Klicken Sie auf „Weiter“, bis Sie eine Datei auswählen können. Wechseln Sie dann zu dem Ort, an dem Sie die Zertifikate erstellt haben, und wählen Sie "server.p12".

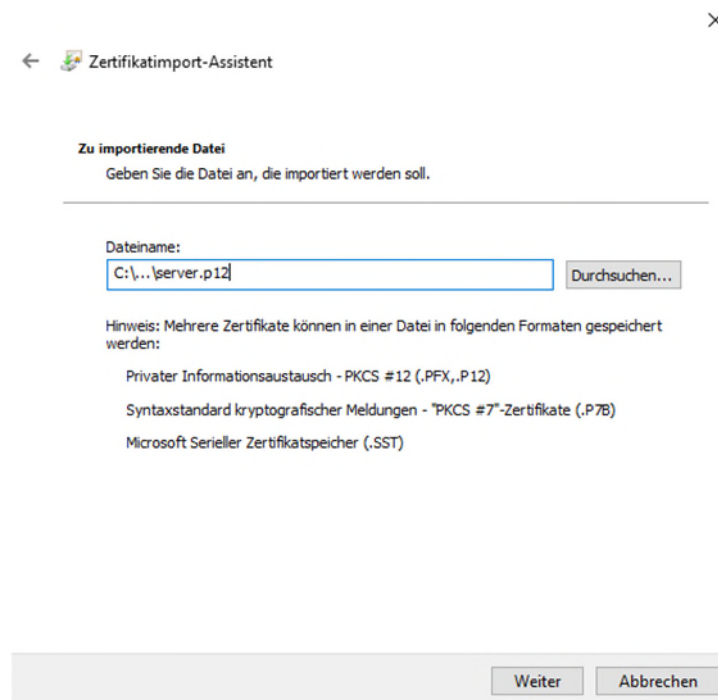


Abbildung 12: Assistent für den Import von Windows-Zertifikaten

5. Das Passwort für die Datei wurde in der Datei "ssl_config.cnf" konfiguriert. Tragen Sie hier Ihr eigenes Passwort ein.
6. Klicken Sie dann auf „Weiter“ -> „Fertig stellen“, um den Import-Assistenten abzuschließen. Es öffnet sich ein Fenster, das bestätigt, dass "der Import erfolgreich war".
7. Nun müssen Sie Firefox die Erlaubnis erteilen, Root-Autoritäten zu vertrauen:

- Type "about: config" into the Firefox address bar.
- Press the **I accept the risk!** button.
- Search for security.enterprise_roots.enabled.



- In the **security.enterprise_roots.enabled** window, look to the right side of the screen. If the value is **False**, double-click on it. The value will get changed to **True**.
- Restart Firefox.

8. Nach erfolgreicher Installation und einem Neustart des Browsers sollte die Verbindung sicher sein:

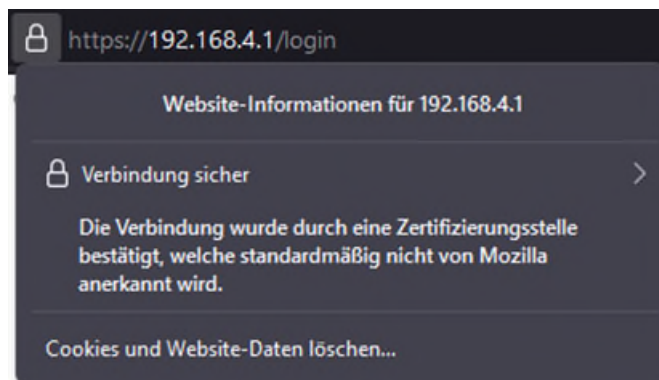


Abbildung 13: Sichere Firefox-Verbindung

14.2.2.3 Chrome und Edge

1. Öffnen Sie Ihren Browser und navigieren Sie zu Einstellungen.
 - Suchen Sie in Chrome nach "Datenschutz und Sicherheit".
 - Gehen Sie in Edge zu "Datenschutz".
2. Klicken Sie auf „Zertifikate verwalten“. Das folgende Fenster wird geöffnet:

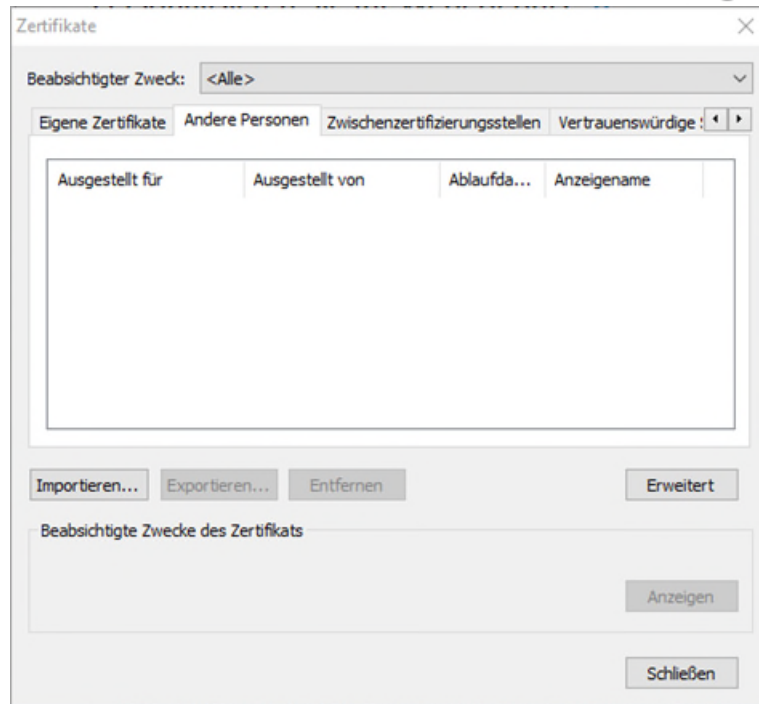


Abbildung 14: Zertifikatsmanager für Chrome und Edge

3. Klicken Sie nun auf „Importieren“ und folgen Sie dem Assistenten.
4. Nach der Auswahl von "server.p12" werden Sie nach einem Passwort gefragt, das in der "ssl_config.cnf" konfiguriert wurde.
5. Starten Sie nach Abschluss des Importassistenten Ihren Browser neu.

14.3 Zertifikat und Schlüssel für MQTT

Für eine sichere TLS-MQTT-Verbindung müssen Sie wie bisher eigene Zertifikate erstellen. Dazu benötigen Sie die Dateien "mqtt_ca_config.cnf" und "ssl_config.cnf", die Sie im [Download-Bereich](#) des ETHERLINE® GUARD finden.

14.3.1 Erstellen mit OpenSSL

Im Folgenden werden neun Dateien erstellt:

- CA-Zertifikat -> für Broker und Client:
 - o "ca.pem", "ca.srl", "cakey.pem"
- MQTT Server Zertifikat und Schlüssel -> für Broker:
 - o "mqttserver.csr", "mqttserver. pem", "mqttserverkey. pem"
- MQTT-Client-Zertifikat und Schlüssel -> für Client:
 - o "mqttclient.csr", "mqttclient.pem", "mqttclientkey.pem"

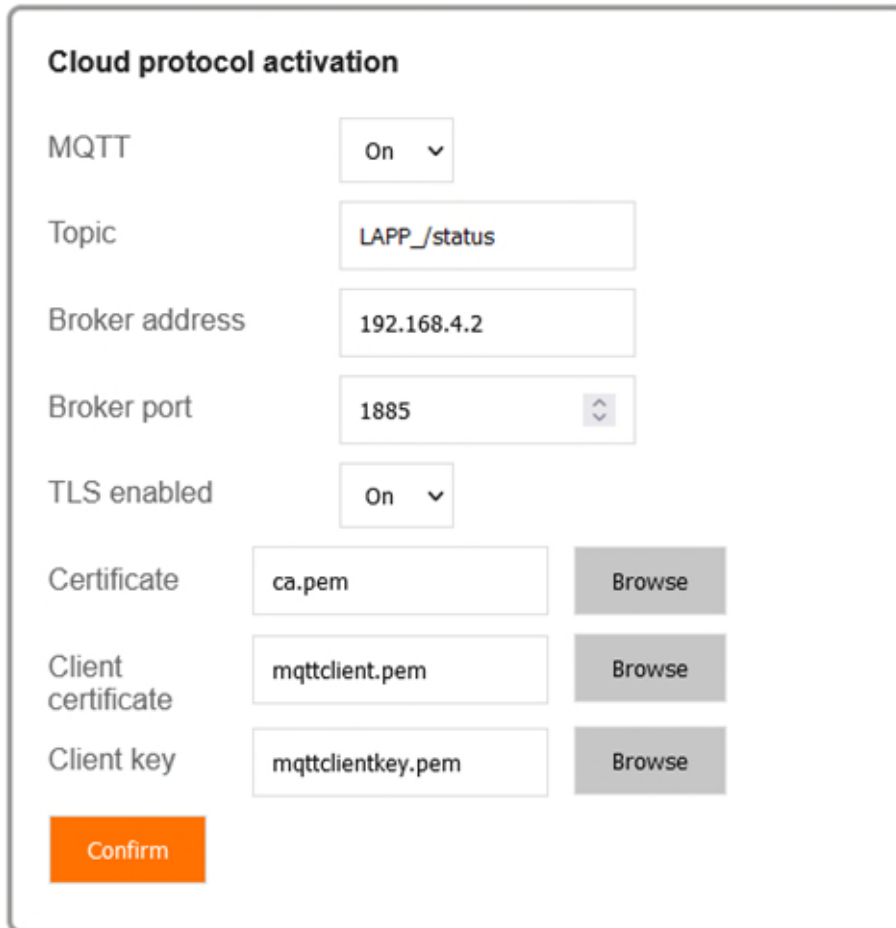
1. Öffnen Sie zunächst Git Bash
2. Wechseln Sie in das Verzeichnis der heruntergeladenen oder selbst erstellten Konfigurationsdatei und geben Sie dann die folgenden Befehle ein:
 - ➔ `openssl req -x509 -nodes -days 7300 -newkey rsa:2048 -keyout cakey.pem -out ca.pem -config mqtt_ca_config.cnf`
 - ➔ `openssl genrsa -out mqttserverkey.pem 2048`

- ➔ `openssl req -new -out mqttserver.csr -key mqttserverkey.pem -config ssl_config.cnf`
- ➔ `openssl x509 -req -in mqttserver.csr -CA ca.pem -CAkey cakey.pem -CAcreateserial -out mqttserver.pem -days 7300`
- ➔ `openssl genrsa -out mqttclientkey.pem 2048`
- ➔ `openssl req -new -out mqttclient.csr -key mqttclientkey.pem -config ssl_config.cnf`
- ➔ `openssl x509 -req -in mqttclient.csr -CA ca.pem -CAkey cakey.pem -CAcreateserial -out mqttclient.pem -days 7300`

14.3.2 Installation von MQTT-Zertifikaten auf dem ETHERLINE® GUARD

Von diesen Dateien müssen Sie das CA-Zertifikat "ca.pem" und das MQTT-Client-Zertifikat und den Schlüssel "mqttclient.pem" und "mqttclientkey.pem" über den Web-Server in Ihren Etherline Guard laden.

1. Öffnen Sie das Webinterface des ETHERLINE® GUARD und navigieren Sie zu Einstellungen
2. Aktivieren Sie unter der Option "Cloud-Protokoll-Aktivierung" TLS. Wenn Sie zuerst eine MQTT-Verbindung konfigurieren wollen, schauen Sie in Kapitel 13 - Anhang A - Einrichten einer MQTT-Verbindung.
3. Wählen Sie die Dateien wie in Abbildung 15:



Cloud protocol activation

MQTT On ▼

Topic

Broker address

Broker port ▼

TLS enabled On ▼

Certificate Browse

Client certificate Browse

Client key Browse

Confirm

Abbildung 15: MQTT-Zertifikat-Installation auf ETHERLINE® GUARD

4. Klicken Sie auf Bestätigen, es erscheint "Einstellungen geändert".