FL MGUARD 1000
Installation und Inbetriebnahme

Anwenderhandbuch

UM DE FL MGUARD 1000

PHOENIX CONTACT
INSPIRING INNOVATIONS

Anwenderhandbuch

FL MGUARD 1000 – Installation und Inbetriebnahme

UM DE FL MGUARD 1000 , Revision 11 2024-05-16

Dieses Handbuch ist gültig für:

Bezeichnung	Revision	Artikel-Nr.
FL MGUARD 1102		1153079
FL MGUARD 1105		1153078

Siehe auch die *mGuardNT 1.8.x Firmware – Release Notes* für weitere Informationen.

108413_de_11

PHOENIX CONTACT GmbH & Co. KG • Flachsmarktstraße 8 • 32825 Blomberg • Germany
phoenixcontact.com

Inhaltsverzeichnis

1 Zu Ihrer Sicherheit

Lesen Sie dieses Handbuch sorgfältig und bewahren Sie es für späteres Nachschlagen auf.

1.1 Kennzeichnung der Warnhinweise

Dieses Symbol mit dem Signalwort **ACHTUNG** warnt vor Handlungen, die zu einem Sachschaden oder einer Fehlfunktion führen können.

Hier finden Sie zusätzliche Informationen oder weiterführende Informationsquellen.

1.2 Über dieses Handbuch

Folgende Elemente werden in diesem Handbuch verwendet:

Fett	Bezeichnung von Bedienelementen, Variablennamen oder sonstige Hervorhebungen
Kursiv	– Produkt-, Modul- oder Komponentenbezeichnungen (z. B. *tftpd64.exe*, *Config API*) – Fremdsprachliche Bezeichnungen oder Eigennamen – Sonstige Hervorhebungen
–	Unnummerierte Aufzählung
1.	Nummerierte Aufzählung
•	Handlungsanweisung
⇒	Ergebnis einer Handlung

1.3 Qualifikation der Benutzer

Der in diesem Handbuch beschriebene Produktgebrauch richtet sich ausschließlich an

– Elektrofachkräfte oder von Elektrofachkräften unterwiesene Personen. Die Anwender müssen vertraut sein mit den einschlägigen Sicherheitskonzepten zur Automatisierungstechnik sowie den geltenden Normen und sonstigen Vorschriften.
– Qualifizierte Anwendungsprogrammierer und Software-Ingenieure. Die Anwender müssen vertraut sein mit den einschlägigen Sicherheitskonzepten zur Automatisierungstechnik sowie den geltenden Normen und sonstigen Vorschriften.

1.4 Bestimmungsgemäße Verwendung

– Die Geräte der Serie FL MGUARD 1000 sind industrietaugliche Security-Router mit integrierter Stateful-Packet-Inspection-Firewall. Sie eignen sich für die dezentrale Absicherung von Produktionszellen oder einzelner Maschinen gegen Manipulationen.
– Das Gerät ist für die Installation im Schaltschrank vorgesehen.

1.5 Veränderung des Produkts

Modifikationen an der Hard- und Firmware des Geräts sind nicht zulässig.

Unsachgemäße Arbeiten oder Veränderungen am Gerät können Ihre Sicherheit gefährden oder das Gerät beschädigen. Sie dürfen das Gerät nicht reparieren. Wenn das Gerät einen Defekt hat, wenden Sie sich an Phoenix Contact.

1.6 Sicherheitshinweise

ACHTUNG: Installation nur durch qualifiziertes Personal

Die Installation, Inbetriebnahme und Wartung des Produkts darf nur durch ausgebildetes Fachpersonal erfolgen, das vom Anlagenbetreiber dazu autorisiert wurde. Elektrofachkraft ist, wer aufgrund seiner fachlichen Ausbildung, Kenntnisse und Erfahrungen sowie Kenntnis der einschlägigen Normen die ihm übertragenen Arbeiten beurteilen und mögliche Gefahren erkennen kann. Das Fachpersonal muss diese Dokumentation gelesen und verstanden haben und die Anweisungen befolgen. Beachten Sie die geltenden nationalen Vorschriften für Betrieb, Funktionsprüfung, Reparatur und Wartung von elektronischen Geräten.

ACHTUNG: Sachschaden durch falsche Beschaltung

Schließen Sie die Netzwerkanschlüsse des Geräts nur an Ethernet-Installationen an. Einige Fernmeldeanschlüsse verwenden ebenfalls RJ45-Buchsen, diese dürfen nicht mit den RJ45-Buchsen des Geräts verbunden werden.

ACHTUNG: Elektrostatische Entladung

Die Geräte enthalten Bauelemente, die durch elektrostatische Entladung beschädigt oder zerstört werden können. Beachten Sie beim Umgang mit den Geräten die notwendigen Sicherheitsmaßnahmen gegen elektrostatische Entladung (ESD) gemäß EN 61340-5-1 und EN 61340-5-2.

ACHTUNG: Anforderung an die Spannungsversorgung

Das Modul ist ausschließlich für den Betrieb mit Sicherheitskleinspannung (SELV/PELV) ausgelegt. Im redundanten Betrieb müssen beide Spannungsversorgungen den Anforderungen der Sicherheitskleinspannung genügen.

ACHTUNG: Anforderung an den Schaltschrank/Schaltkasten

Dieses Modul wird innerhalb eines Schaltschranks oder -kastens auf eine Norm-Tragschiene aufgerastet. Dieser Schaltschrank/-kasten muss den Anforderungen der IEC/EN 62368-1 bez. der Brandschutzumhüllung genügen.

ACHTUNG: Anforderung an die Funktionserdung

Montieren Sie das Modul auf einer geerdeten Tragschiene. Die Erdung des Moduls erfolgt mit dem Aufrasten auf die Tragschiene.

ACHTUNG: Anforderung an den Montageort

Die vorgeschriebene Einbaulage ist senkrecht auf einer horizontal montierten Tragschiene. Die Lüftungsschlitze dürfen nicht bedeckt werden, so dass die Luft frei zirkulieren kann. Als Abstand zu den Lüftungsschlitzen des Gehäuses werden mindestens 3 cm empfohlen.

Öffnen oder Verändern des Gerätes ist nicht zulässig. Reparieren Sie das Gerät nicht selbst, sondern ersetzen Sie es durch ein gleichwertiges Gerät. Reparaturen dürfen nur vom Hersteller vorgenommen werden. Der Hersteller haftet nicht für Schäden aus Zuwiderhandlung.

Die Schutzart IP20 (IEC 60529-0/EN 60529-0) des Gerätes ist für eine saubere und trockene Umgebung vorgesehen. Setzen Sie das Gerät keiner mechanischen und/oder thermischen Beanspruchung aus, die die beschriebenen Grenzen überschreitet.

ACHTUNG: Beachten Sie beim Einsatz des Geräts folgende Sicherheitshinweise.

- Halten Sie die für das Errichten und Betreiben geltenden Bestimmungen und Sicherheitsvorschriften (auch nationale Sicherheitsvorschriften) sowie die allgemeinen Regeln der Technik ein.
- Die technischen Daten sind der Packungsbeilage und den Zertifikaten (Konformitätsbewertung, ggf. weitere Approbationen) zu entnehmen.
- Setzen Sie das Gerät keinem direktem Sonnenlicht oder dem direkten Einfluss einer Wärmequelle aus, um eine Überhitzung zu vermeiden.
- Verwenden Sie zum Reinigen des Gerätegehäuses ein weiches Tuch. Verwenden Sie keine aggressiven Lösungsmittel.

1.7 IT-Sicherheit

Sie müssen Komponenten, Netzwerke und Systeme vor unberechtigten Zugriffen schützen und die Datenintegrität gewährleisten. Hierzu müssen Sie bei netzwerkfähigen Geräten, Lösungen und PC-basierter Software organisatorische und technische Maßnahmen ergreifen.

Phoenix Contact empfiehlt dringend den Einsatz eines Managementsystems für Informationssicherheit (ISMS) zur Verwaltung aller infrastrukturellen, organisatorischen und personellen Maßnahmen, die zur Erhaltung der Informationssicherheit notwendig sind.

Darüber hinaus empfiehlt Phoenix Contact, mindestens die folgenden Maßnahmen zu berücksichtigen.

Weiterführende Informationen zu den im Folgenden genannten Maßnahmen erhalten Sie auf den folgenden Webseiten (letzter Zugriff am 15.04.2024):

bsi.bund.de/it-sik.html

ics-cert.us-cert.gov/content/recommended-practices

Verwenden Sie die jeweils aktuelle Firmware-Version

Phoenix Contact stellt regelmäßig Firmware-Updates zur Verfügung. Verfügbare Firmware-Updates finden Sie auf der Produktseite des jeweiligen Geräts.

- Stellen Sie sicher, dass die Firmware aller verwendeten Geräte immer auf dem aktuellen Stand ist.
- Beachten Sie die Change Notes / Release Notes zur jeweiligen Firmware-Version.
- Beachten Sie die Webseite des Product Security Incident Response Teams (PSIRT) von Phoenix Contact für Sicherheitshinweise zu veröffentlichten Sicherheitslücken.

Verwenden Sie aktuelle Sicherheits-Software

- Um Sicherheitsrisiken wie Viren, Trojaner und andere Schad-Software zu erkennen und auszuschalten, installieren Sie auf allen PCs eine Sicherheits-Software.
- Stellen Sie sicher, dass die Sicherheits-Software immer auf dem aktuellen Stand ist und die neuesten Datenbanken nutzt.
- Nutzen Sie Whitelist-Tools zur Überwachung des Gerätekontexts.
- Um die Kommunikation Ihrer Anlage zu prüfen, nutzen Sie ein Intrusion-Detection-System.

Führen Sie regelmäßige Bedrohungsanalysen durch

- Um festzustellen, ob die von Ihnen getroffenen Maßnahmen Ihre Komponenten, Netzwerke und Systeme noch ausreichend schützen, ist eine regelmäßige Bedrohungsanalyse erforderlich.
- Führen Sie regelmäßige Bedrohungsanalysen durch.

Berücksichtigen Sie bei der Anlagenplanung Defense-in-depth-Mechanismen

Um Ihre Komponenten, Netzwerke und Systeme zu schützen, ist es nicht ausreichend, isoliert betrachtete Maßnahmen zu ergreifen. Defense-in-Depth-Mechanismen umfassen mehrere, aufeinander abgestimmte und koordinierte Maßnahmen, die Betreiber, Integratoren und Hersteller miteinbeziehen.

- Berücksichtigen Sie bei der Anlagenplanung Defense-in-depth-Mechanismen

Deaktivieren Sie nicht benötigte Kommunikationskanäle

- Deaktivieren Sie nicht benötigte Kommunikationskanäle (z. B. SNMP, FTP, BootP, DCP etc.) an den von Ihnen eingesetzten Komponenten.

Binden Sie Komponenten und Systeme nicht in öffentliche Netzwerke ein

- Vermeiden Sie es, Ihre Komponenten und Systeme in öffentliche Netzwerke einzubinden.
- Wenn Sie Ihre Komponenten und Systeme über ein öffentliches Netzwerk erreichen müssen, verwenden Sie ein VPN (Virtual Private Network).

Beschränken Sie die Zugangsberechtigung zum Gerät

- Vermeiden Sie, dass unberechtigte Personen physischen Zugriff auf das Gerät erlangen. Ein Zugriff auf die Hardware des Geräts könnte es einem Angreifer ermöglichen, die Sicherheitsfunktionen zu manipulieren.
- Beschränken Sie die Zugangsberechtigung zu Komponenten, Netzwerken und Systemen auf die Personen, für die eine Berechtigung unbedingt notwendig ist.
- Deaktivieren Sie nicht genutzte Benutzerkonten.

Sichern Sie den Zugriff ab

- Ändern Sie voreingestellte Passwörter während der ersten Inbetriebnahme.
- Verwenden Sie sichere Passwörter, deren Komplexität und Lebensdauer dem Stand der Technik entsprechen (z. B. mit einer Länge von mindestens zehn Zeichen und einer Mischung aus Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen).
- Verwenden Sie Passwort-Manager mit zufällig erzeugten Passwörtern.
- Ändern Sie Passwörter entsprechend der für Ihre Anwendung geltenden Regeln.
- Verwenden Sie, sofern möglich, zentrale Benutzerverwaltungen zur Vereinfachung des User Managements und der Anmeldeinformationen.

Verwenden Sie bei Fernzugriff sichere Zugriffswege

- Verwenden Sie für einen Fernzugriff sichere Zugriffswege wie VPN (Virtual Private Network) oder HTTPS.

Verwenden Sie eine Firewall

- Richten Sie eine Firewall ein, um Ihre Netzwerke und darin eingebundene Komponenten und Systeme vor ungewollten Netzwerkzugriffen zu schützen.
- Verwenden Sie eine Firewall, um ein Netzwerk zu segmentieren oder bestimmte Komponenten (z. B. Steuerungen) zu isolieren.

Aktivieren Sie eine sicherheitsrelevante Ereignisprotokollierung (Logging)

- Aktivieren Sie die sicherheitsrelevante Ereignisprotokollierung (Logging) gemäß der Sicherheitsrichtlinie und der gesetzlichen Bestimmungen zum Datenschutz.

Schützen Sie den Zugriff auf die SD-Karte

Geräte mit SD-Karten benötigen Schutz gegen unerlaubte physische Zugriffe. Eine SD-Karte kann mit einem herkömmlichen SD-Kartenleser jederzeit ausgelesen werden. Wenn Sie die SD-Karte nicht physisch gegen unbefugte Zugriffe schützen (z. B. mithilfe eines gesicherten Schaltschranks), sind somit auch sensible Daten für jeden abrufbar.

- Stellen Sie sicher, dass Unbefugte keinen Zugriff auf die SD-Karte haben.
- Stellen Sie bei der Vernichtung der SD-Karte sicher, dass die Daten nicht wiederhergestellt werden können.

1.8 Aktuelle Sicherheitshinweise zu Ihrem Produkt

Product Security Incident Response Team (PSIRT)

Das Phoenix Contact PSIRT ist das zentrale Team für Phoenix Contact und dessen Tochterunternehmen, dessen Aufgabe es ist, auf potenzielle Sicherheitslücken, Vorfälle und andere Sicherheitsprobleme im Zusammenhang mit Produkten, Lösungen sowie Diensten von Phoenix Contact zu reagieren.

Das Phoenix Contact PSIRT leitet die Offenlegung, Untersuchung und interne Koordination und veröffentlicht Sicherheitshinweise zu bestätigten Sicherheitslücken, bei denen Maßnahmen zur Abschwächung oder Behebung verfügbar sind.

Die PSIRT-Webseite (phoenixcontact.com/psirt) wird regelmäßig aktualisiert. Zusätzlich empfiehlt Phoenix Contact, den PSIRT-Newsletter zu abonnieren.

Jeder kann per E-Mail Informationen zu potenziellen Sicherheitslücken beim Phoenix Contact PSIRT einreichen.

1.9 Support

Zusätzliche Informationen zum Gerät sowie Release Notes, Anwenderhilfen und Software-Updates finden Sie unter folgender Internet-Adresse:
phoenixcontact.net/product/<Artikelnummer>.

Bei Problemen mit Ihrem Gerät oder der Bedienung Ihres Geräts wenden Sie sich bitte an Ihre Bezugsquelle.

Um in einem Fehlerfall schnelle Hilfe zu erhalten, erstellen Sie, falls möglich, beim Auftreten des Fehlers umgehend einen Snapshot der Gerätekonfiguration, den Sie dem Support zur Verfügung stellen können.

Die Verwendung von Snapshots wird im Anwenderhandbuch „*FL MGUARD 1000 – Web-based Management*“ (UM DE MGUARD NT) beschrieben. Erhältlich im Download-Bereich der entsprechenden Produktseite im Phoenix Contact Web-Shop, z. B. unter phoenixcontact.net/product/1153079.

2 Gerätebeschreibung

Die Geräte der Serie FL MGUARD 1000 sind industrietaugliche Security-Router mit integrierter Stateful-Packet-Inspection-Firewall. Sie ermöglichen einen hohen Datendurchsatz im Gigabit-Bereich und eignen sich für die dezentrale Absicherung von Produktionszellen oder einzelner Maschinen gegen Manipulationen.

NAT-Router

Als Router bzw. Gateway verbindet das Gerät Subnetze bzw. Netzzonen. Für jede Netzzone ist eine eigene IP-Adresse konfiguriert, über die das Gerät im Netzwerk erreichbar ist.

Über die NAT-Funktionen (IP-Masquerading, 1:1-NAT, Port-Weiterleitung) können einzelne Maschinen (SPS) oder mehrere Subnetze mit gleicher IP-Konfiguration leicht in ein bestehendes Netzwerk eingebunden werden, ohne dass die IP-Konfiguration der Maschine bzw. der Subnetze geändert werden muss.

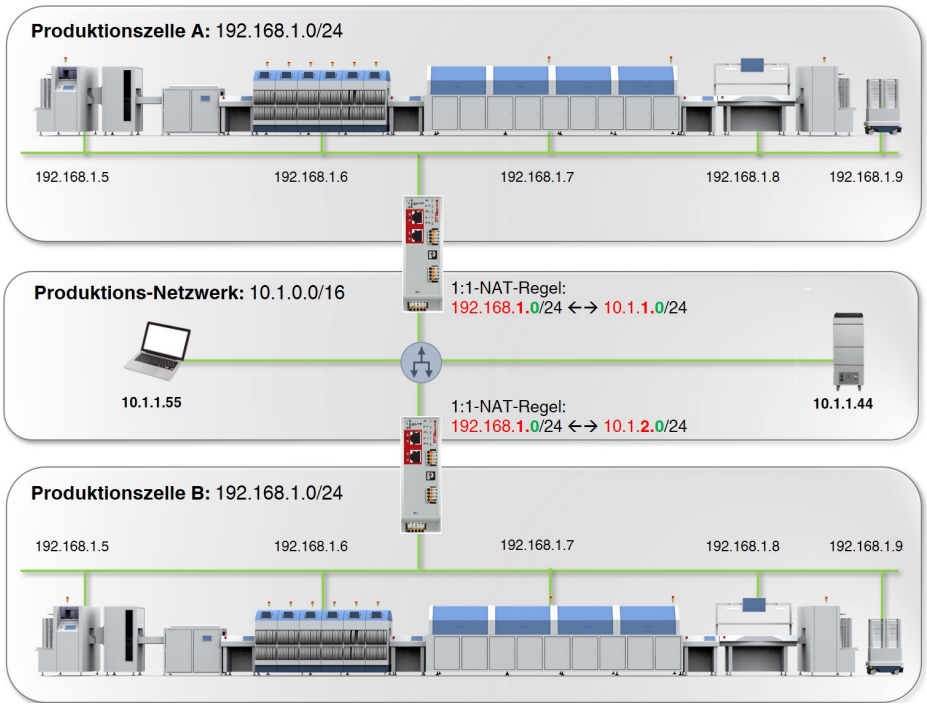


Bild 2-1 NAT-Router

Security by Design

Alle mGuard-Geräte verfügen über die bewährte *mGuard Security Technology* und wurden damit von Grund auf nach den Anforderungen für Netzwerksicherheit entwickelt. Die Geräte nutzen eine leistungsfähige Firewall. System- und Netzwerkdienste wurden gehärtet.

Sicherheitslücken - schnell geschlossen (PSIRT)

Über den PSIRT-Prozess (*Product Security Incident Response Team*) werden alle verwendeten Komponenten kontinuierlich überwacht. Entdeckte oder gemeldete Sicherheitslücken werden umgehend analysiert und, falls erforderlich, geschlossen (siehe PSIRT).

Durch die integrierte *mGuard Security Technology* sorgen die Geräte für eine dezentrale Absicherung von Produktionszellen oder einzelnen Maschinen gegen Manipulationen.

2.1 Produktübersicht

Tabelle 2-1 Produktübersicht und Artikelnummern

Gerät	Kurzbeschreibung	Artikelnummer
FL MGUARD 1102	2 x RJ45-Ports, SD-Kartenhalter, digitale Service I/Os	1153079
FL MGUARD 1105	5 x RJ45-Ports, SD-Kartenhalter, digitale Service I/Os	1153078

2.2 Lieferumfang

Das Gerät wird in einer Verpackung zusammen mit einer Packungsbeilage mit Einbauhinweisen geliefert.

- Lesen Sie die Packungsbeilage aufmerksam durch.
- Bewahren Sie die Packungsbeilage auf.

2.2.1 Lieferung kontrollieren

- Prüfen Sie die Lieferung auf Transportschäden.

  Jede Beschädigung der Verpackung ist ein Hinweis auf einen möglichen transportbedingten Schaden des Geräts. Ein Funktionsausfall kann möglich sein.
- Prüfen Sie den Verpackungsinhalt unmittelbar nach Anlieferung anhand des Lieferscheins auf Vollständigkeit.
- Reklamieren Sie entstandene Transportschäden sofort und informieren Sie umgehend Phoenix Contact oder Ihren Lieferanten sowie das Transportunternehmen.
- Fügen Sie Ihrer Reklamation aussagekräftige Fotos der beschädigten Verpackung/der beschädigten Lieferung bei.
- Bewahren Sie Versandkartons und Verpackungsmaterial zwecks möglicher Rücksendung auf.
- Verwenden Sie bei Rücksendung vorzugsweise die Originalverpackung.
- Beachten Sie die Hinweise in Kapitel 6, falls die Originalverpackung nicht mehr vorliegt.

2.3 FL MGUARD 1102

Das Gerät verfügt über folgende Netzwerkanschlüsse:

– **Netzwerkinterface / Netzzone 1**: Ethernet 10/100/1000 Mbit/s (RJ45-Port)
– **Netzwerkinterface / Netzzone 2**: Ethernet 10/100/1000 Mbit/s (RJ45-Port)

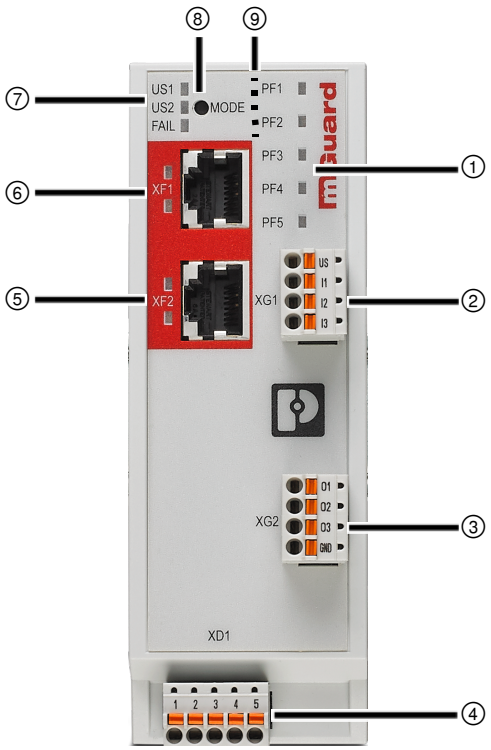


Bild 2-2 FL MGUARD 1102: Bedienelemente und Anzeigen

① Status- und Diagnose-LEDs
(siehe Kapitel 2.5.1)

② Anschluss digitaler **Eingänge** über COMBICON-Steckverbindung (Push-in-Kontakt)
(siehe Kapitel 3.4)

③ Anschluss digitaler **Ausgänge** über COMBICON-Steckverbindung (Push-in-Kontakt)
(siehe Kapitel 3.4)

④ Anschluss der Versorgungsspannung über COMBICON-Steckverbindung (Push-in-Kontakt)
(siehe Kapitel 3.2)

⑤ Netzwerkinterface / Netzzone 2 (RJ45-Ethernet-Port) (siehe Kapitel 3.3)
LED LNK/ACT (oben) | LED SPD (unten)
(siehe Kapitel 2.5.2)

⑥ Netzwerkinterface / Netzzone 1 (RJ45-Ethernet-Port) (siehe Kapitel 3.3)
LED LNK/ACT (oben) | LED SPD (unten)
(siehe Kapitel 2.5.2)

⑦ Status- und Diagnose-LEDs
(siehe Kapitel 2.5.3, 2.5.4)

⑧ Mode-Taste
(siehe Kapitel 5)

⑨ SD-Kartenhalter (auf der Rückseite des Geräts)
(siehe Kapitel 3.5)

2.4 FL MGUARD 1105

Das Gerät verfügt über folgende Netzwerkanschlüsse:

– **Netzwerkinterface / Netzzone 1**: Ethernet 10/100/1000 Mbit/s (RJ45-Port)
– **Netzwerkinterface / Netzzone 2**: 4-Port-Ethernet-Switch: 10/100/1000 Mbit/s (RJ45-Port)

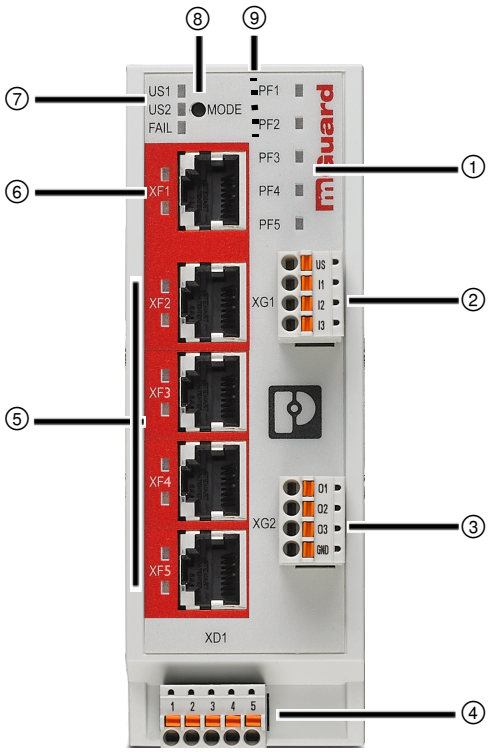


Bild 2-3 FL MGUARD 1105: Bedienelemente und Anzeigen

① Status- und Diagnose-LEDs
(siehe Kapitel 2.5.1)

② Anschluss digitaler Eingänge über COMBICON-Steckverbindung (Push-in-Kontakt)
(siehe Kapitel 3.4)

③ Anschluss digitaler Ausgänge über COMBICON-Steckverbindung (Push-in-Kontakt)
(siehe Kapitel 3.4)

④ Anschluss der Versorgungsspannung über COMBICON-Steckverbindung (Push-in-Kontakt)
(siehe Kapitel 3.2)

⑤ Netzwerkinterface / Netzzone 2 (4x RJ45-Ethernet-Port) (siehe Kapitel 3.3)
LED LNK/ACT (oben) | LED SPD (unten)
(siehe Kapitel 2.5.2)

⑥ Netzwerkinterface / Netzzone 1 (RJ45-Ethernet-Port) (siehe Kapitel 3.3)
LED LNK/ACT (oben) | LED SPD (unten)
(siehe Kapitel 2.5.2)

⑦ Status- und Diagnose-LEDs
(siehe Kapitel 2.5.3, 2.5.4)

⑧ Mode-Taste
(siehe Kapitel 5)

⑨ SD-Kartenhalter (auf der Rückseite des Geräts)
(siehe Kapitel 3.5)

2.5 LED – Status- und Diagnoseanzeige

Mithilfe der Status- und Diagnose-LEDs werden unterschiedliche System- und Fehlerzustände des Geräts angezeigt.

2.5.1 PF1 – PF5

Die dreifarbigen LEDs PF1 – PF5 (grün/rot/orange) zeigen verschiedene Status und Systemzustände des Geräts an.

Sie kommen u. a. bei der Verwendung des Smart-Mode zum Einsatz (siehe Tabelle 2-3).

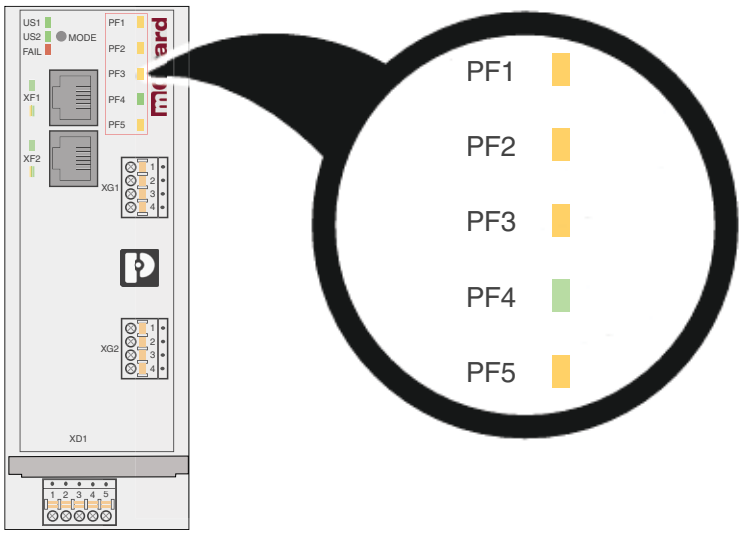
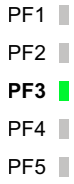


Bild 2-4 LEDs: PF1 – PF5

Tabelle 2-2 LEDs: PF1 – PF5: Geräte-Status

Geräte-Status				Geräte-Fehler
Wird gestartet	**Firmware-Update**	**Betriebsbereit**	**Test-Mode-Alarm**	**Import von SD-Karte fehlgeschlagen**
PF1 ■ PF2 ■ PF3 ■ PF4 ■ PF5 ■	PF1 ■ PF2 ■ PF3 ■ PF4 ■ PF5 ■	PF1 ✦■ PF2 ■ PF3 ■ PF4 ■ PF5 ■	PF1 ✦■ PF2 ■ PF3 ■ PF4 ■ PF5 ■	PF1 ■ PF2 ■ PF3 ■ PF4 ■ PF5 ■
Warten Sie, bis das Gerät vollständig gestartet wurde.	Die Firmware wird auf das Gerät geschrieben. **ACHTUNG: Eine Unterbrechung der Stromversorgung kann das Gerät beschädigen!** **Schalten Sie das Gerät nicht aus!** Warten Sie, bis das Gerät vollständig gestartet wurde.	Das Gerät wurde vollständig gestartet. Die LED PF1 blinkt im Rhythmus eines Herzschlags.	Der Firewall-Test-Mode ist aktiv und hat einen oder mehrere Alarme ausgelöst. Die LED PF1 blinkt im Rhythmus eines Herzschlags.	Der Versuch, eine Konfiguration von SD-Karte in das Gerät zu laden und anzuwenden, ist fehlgeschlagen. Das Gerät wird mit den Werkseinstellungen gestartet. Die LED FAIL leuchtet zusätzlich permanent rot.

Tabelle 2-3 LEDs: PF1 – PF5: Smart-Mode

Smart-Mode-Funktion (siehe Kapitel 5.1)			
Ausgewählt **(Beispiel)**	**Wird ausgeführt** **(Beispiel)**	**Erfolgreich beendet**	**Fehlgeschlagen**
			
Die LED zeigt an, welche Smart-Mode-Funktion ausgewählt wurde (siehe Tabelle 5-1). Zusätzlich blinken PF1–5 alle vier Sekunden simultan dreimal grün.	Die Smart-Mode-Funktion wird ausgeführt. Schalten Sie das Gerät nicht aus. **ACHTUNG: Eine Unterbrechung der Stromversorgung kann das Gerät beschädigen!** **Schalten Sie das Gerät nicht aus!** Warten Sie, bis die Smart-Mode-Funktion erfolgreich beendet wurde.	Die Smart-Mode-Funktion wurde erfolgreich ausgeführt. Starten Sie das Gerät neu.	Starten Sie im Fehlerfall das Gerät neu und wenden Sie sich im weiteren Fehlerfall an Ihren Support. Ein schwerwiegender Fehler kann auch durch die LED „FAIL“ angezeigt werden.

2.5.2 LNK/ACT und SPD

Die LEDs LNK/ACT (*Link/Activity)* und SPD (*Speed*) zeigen den Status der Netzwerkverbindung des zugehörigen Netzwerkports an (siehe Tabelle 2-4).

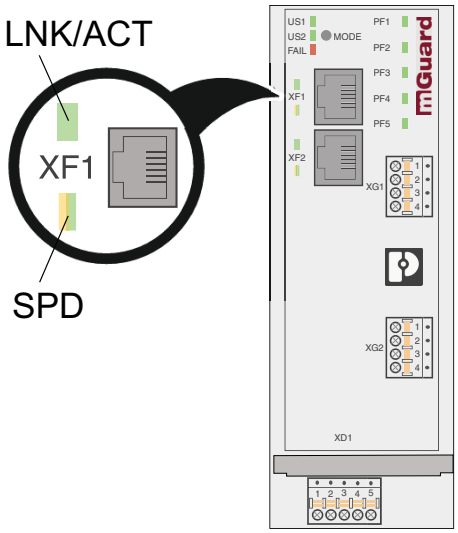


Bild 2-5 LEDs: LNK/ACT und SPD

Tabelle 2-4 LEDs: LNK/ACT und SPD

Bezeichnung	Farbe	Status	Bedeutung
LNK/ACT (XF1–XF5) (obere LED)	Grün	An	Link aktiv
		Blinken	Datenpakete werden übertragen.
		Aus	Link nicht aktiv
SPD (XF1–XF5) (untere LED)	Grün/Orange	An (orange)	1000 Mbit/s (Gigabit Ethernet)
		An (grün)	100 Mbit/s (Fast Ethernet)
		Aus	10 Mbit/s (Ethernet) (wenn LED LNK/ACT aktiv)
		Aus	Keine Datenübertragung (wenn LED LNK/ACT inaktiv)

2.5.3 US1 und US2

Die LEDs US1 und US2 zeigen den Status der Spannungsversorgung des Geräts an.

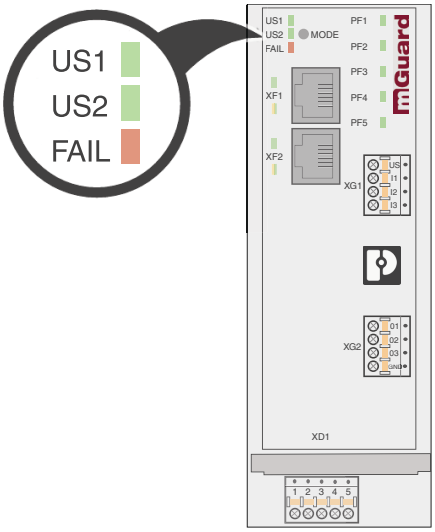


Bild 2-6 LEDs: US1, US2

Tabelle 2-5 LEDs: US1, US2

Bezeichnung	Farbe	Status	Bedeutung
US1	Grün	An	Versorgungsspannung liegt im Toleranzbereich (siehe Kapitel 5)
		Aus	Versorgungsspannung nicht vorhanden oder zu niedrig (siehe Kapitel 5)
US2	Grün	An	Die Geräte verfügen über keine redundante Spannungsversorgung.
		Aus	

2.5.4 FAIL

Die LED FAIL zeigt verschiedene Status und Fehlerzustände des Geräts an.

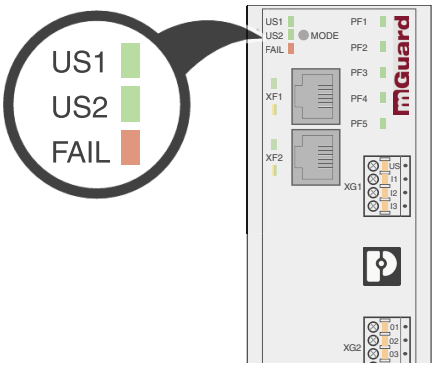


Bild 2-7 LED: FAIL

Tabelle 2-6 LED: FAIL

Bezeichnung	Farbe	Status	Bedeutung
FAIL	Rot	An (kurz)	Das Gerät wird neu gestartet. • Warten Sie, bis die Betriebsbereitschaft des Geräts hergestellt wurde (siehe Kapitel 4.3.1). ⇒ Das Gerät ist betriebsbereit, wenn PF2–PF5 erloschen sind und PF1 grün blinkt (Herzschlag).
		An (permanent)	Ein schwerwiegender Fehler liegt vor. ⇒ Die Betriebsbereitschaft des Geräts wurde nicht erreicht. ⇒ Alle Netzwerkinterfaces sind deaktiviert. • Starten Sie das Gerät neu.
		An (permanent) + LED PF1 (rot)	Die LED PF1 leuchtet zusätzlich rot: ⇒ Der Versuch, eine Konfiguration von SD-Karte in das Gerät zu laden und anzuwenden, ist fehlgeschlagen. ⇒ Das Gerät wird mit den Werkseinstellungen gestartet.
		An (blinken)	Ein schwerwiegender Fehler liegt vor. ⇒ Die Betriebsbereitschaft des Geräts wurde nicht erreicht. ⇒ Alle Netzwerkinterfaces sind deaktiviert. • Starten Sie das Gerät neu.
		Kontaktieren Sie gegebenenfalls Ihren Support (siehe Kapitel 1.9).	

2.6 Werkseinstellungen

In den Werkseinstellungen (Auslieferungszustand) ist das Gerät wie nachfolgend beschrieben konfiguriert.

2.6.1 Netzwerkinterfaces

Die grundlegenden Netzwerkfunktionen (Ethernet) des Geräts sind nach dem Start des Geräts verfügbar (siehe Tabelle 2-7).

Tabelle 2-7 **Werkseinstellungen**: Konfiguration der Netzwerkinterfaces

Funktion	Netzzone 1 (XF1)	Netzzone 2 (XF2–XF5) (*Bridge Mode*)
IP-Adresse (IPv4)	Wird automatisch zugewiesen, wenn ein DHCP-Server im Netzwerk vorhanden ist.	192.168.1.1
Netzmaske		24
Standard-Gateway	Kann automatisch zugewiesen werden, wenn ein DHCP-Server im Netzwerk vorhanden ist.	–
IP-Masquerading (NAT)	Wird auf alle gerouteten Datenpakete angewendet, die das Gerät über das Netzwerkinterface XF1 (nach Netzzone 1) verlassen.	–

2.6.2 Benutzerzugriff

Der Zugriff auf die Benutzerinterfaces WBM und *Config API* erfolgt unter der Angabe von Benutzername und Passwort.

– **Benutzername**: *admin*
– **Passwort**: *private*

Ändern Sie bei der Erstinbetriebnahme des Geräts umgehend das voreingestellte Administrator-Passwort.

Der Netzwerkzugriff auf das Gerät ist darüber hinaus durch die Firewall für eingehenden Datenverkehr beschränkt (siehe „Firewall (für eingehenden Datenverkehr) = Gerätezugriff“)

2.6.3 Aktive Netzwerkdienste (Gerät als Client)

Folgende Netzwerkdienste sind auf dem Gerät (als Client) in den Werkseinstellungen aktiviert.

Tabelle 2-8 **Werkseinstellungen**: Aktive Dienste (als Client)

Dienst/Service	Aktiv über	Konfiguration (Werkseinstellungen)
DHCP-Client	Netzzone 1 (XF1)	Sendet DHCP-Anfragen an erreichbare DHCP-Server in seinem Netzwerk über UDP-Port 67.
DNS-Client	Netzzone 1 (XF1) (Netzzone 2 [XF2–XF5] übernimmt die Einstellungen von Netzzone 1)	Sendet DNS-Anfragen an verfügbare DNS-Server über UDP-Port 53. Werkseinstellungen: Die Adresse eines DNS-Servers kann per DHCP zugewiesen worden sein, wenn ein DHCP-Server im Netzwerk vorhanden ist. Für den Fall, dass keine Adresse per DHCP zugewiesen wurde, werden die im Gerät voreingestellten *Root Name Server* verwendet.
NTP-Client	Netzzone 1 (XF1) Netzzone 2 (XF2–XF5)	Sendet NTP-Anfragen an verfügbare NTP-Server über UDP-Port 123. Werkseinstellungen: Die folgenden Adressen (Hostnamen) der NTP-Server sind voreingestellt: – 0.pool.ntp.org – 1.pool.ntp.org – 2.pool.ntp.org – 3.pool.ntp.org

2.6.4 Aktive Netzwerkdienste (Gerät als Server)

Folgende Netzwerkdienste sind auf dem Gerät (als Server) in den Werkseinstellungen aktiviert und über die Netzwerkinterfaces von außen erreichbar.

Tabelle 2-9 **Werkseinstellungen**: Aktive Dienste (als Server)

Dienst/Service	Erreichbar über	Konfiguration (Werkseinstellungen)
Webserver	Netzzone 2 (XF2–XF5)	Anfrage über TCP-Port 443 (HTTPS) Clients, die über Netzzone 2 mit dem Gerät verbunden sind, können auf das Web-based Management (WBM) zugreifen.
RESTful Server	Netzzone 2 (XF2–XF5)	Anfrage über TCP-Port 443 (HTTPS) Clients, die über Netzzone 2 mit dem Gerät verbunden sind, können auf den RESTful-Server (*Config API*) zugreifen.
SNMP-Server	Netzzone 2 (XF2–XF5)	Anfrage über UDP-Port 161 (SNMP) Clients, die über Netzzone 2 mit dem Gerät verbunden sind, können lesend auf den SNMP-Server zugreifen.
DHCP-Server	Netzzone 2 (XF2–XF5)	Anfrage über UDP-Port 67 Clients, die über Netzzone 2 mit dem Gerät verbunden sind, können eine Netzwerkkonfiguration von dessen DHCP-Server anfordern. Folgende Netzwerkkonfiguration wird an anfragende Clients vergeben: – IP-Adresse aus dem Bereich: 192.168.1.2 ... 192.168.1.254 – Lokale Netzmaske: 24 – Standard-Gateway: 192.168.1.1 – DNS-Server: 192.168.1.1
DNS-Server	Netzzone 2 (XF2–XF5)	Anfrage über UDP- und TCP-Port 53 Clients, die über Netzzone 2 mit dem Gerät verbunden sind, können Anfragen zur Namensauflösung an dessen DNS-Server senden.
NTP-Server	Netzzone 2 (XF2–XF5)	Anfrage über UDP-Port 123 Clients, die über Netzzone 2 mit dem Gerät verbunden sind, können ihre Systemzeit über den NTP-Server des Geräts synchronisieren.

2.6.5 Firewall und Gerätezugriff

Bei der Firewall wird grundsätzlich zwischen eingehendem und durchgehendem (*geroutetem*) Datenverkehr unterschieden:

– **Eingehender Datenverkehr** bezieht sich auf die Pakete, die an das Gerät gesendet werden (Gerätezugriff).
– **Durchgehender Datenverkehr** bezieht sich auf die Pakete, die durch das Gerät durchgeleitet (*geroutet*) werden, z. B. eingehend über Netzzone 2 (XF2–XF5) und ausgehend über Netzzone 1 (XF1).

Firewall (für eingehenden Datenverkehr) = Gerätezugriff

Tabelle 2-10 **Werkseinstellungen**: Firewall für eingehenden Datenverkehr

Dienst/ Service, Protokoll	Eingehend über	Port	Beschreibung
HTTPS	Netzzone 2 (XF2–XF5)	TCP 443	Entsprechende Anfragen an den Webserver des Geräts sind erlaubt. Unter anderem: – Anmeldung und Konfiguration via Web-based Management – Anmeldung und Konfiguration via RESTful-Server (*Config API*)
SNMP	Netzzone 2 (XF2–XF5)	UDP 161	Entsprechende Anfragen an den SNMP-Server des Geräts sind erlaubt.
DHCP	Netzzone 2 (XF2–XF5)	UDP 67	Entsprechende Anfragen an den DHCP-Server des Geräts sind erlaubt.
DNS	Netzzone 2 (XF2–XF5)	TCP 53 UDP 53	Entsprechende Anfragen an den DNS-Server des Geräts sind erlaubt.
NTP	Netzzone 2 (XF2–XF5)	UDP 123	Entsprechende Anfragen an den NTP-Server des Geräts sind erlaubt.
ICMP **(IPv4)**	Netzzone 1 (XF1) Netzzone 2 (XF2–XF5)		Ping-Anfragen (*ICMP requests*) an die konfigurierten oder per DHCP zugewiesenen IPv4-Adressen der Netzzonen (im Router-Modus) oder die Management-IP-Adresse (im Stealth-Modus) sind erlaubt.

Zugriffe auf alle anderen Netzwerkdienste und Netzwerkprotokolle des Geräts werden von der Firewall verworfen.

Werkseinstellungen: Firewall (für durchgehenden Datenverkehr) = Routing
Alle Pakete, die aus der Netzzone 2 (XF2–XF5), also aus dem Subnetzwerk 192.168.1.0/24, an beliebige Zieladressen gesendet werden, werden vom Gerät weitergeleitet (*geroutet*).

Alle anderen Pakete werden verworfen.

3 Montage und Installation

3.1 Montieren und demontieren

ACHTUNG: Gerätebeschädigung
Montieren und demontieren Sie das Gerät nur im spannungsfreien Zustand.

Das Gerät ist zur Installation in einem Schaltschrank vorgesehen. Montieren Sie das Gerät auf einer sauberen Tragschiene nach DIN EN 50 022.

Gerät montieren

- Setzen Sie das Modul von oben auf die Tragschiene (**A**). Dabei muss die obere Haltenut des Moduls mit der Oberkante der Tragschiene verhaken.
- Drücken Sie das Modul an der Front in Richtung der Montagefläche (**B**).
- Nachdem das Modul hörbar eingerastet hat, prüfen Sie den festen Sitz des Geräts.
- Verbinden Sie die Tragschiene mit der Schutzerde.

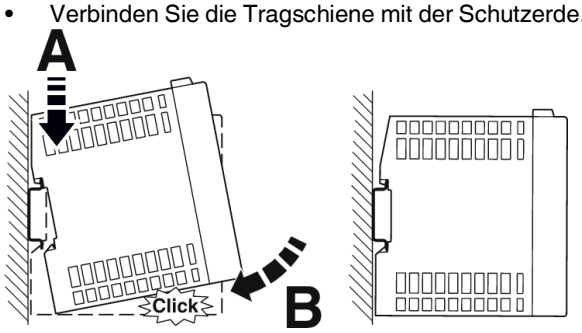


Bild 3-1 Aufrasten des Geräts auf eine Tragschiene

Gerät demontieren

- Ziehen Sie die Rastlasche (**A**) mit einem geeigneten Werkzeug (z. B. Schraubendreher) nach unten (**B**). Die Rastlasche verbleibt im ausgerasteten Zustand.
- Schwenken Sie die Unterseite des Geräts etwas von der Tragschiene weg (**C**).
- Heben Sie das Gerät nach oben hin von der Tragschiene weg (**D**).

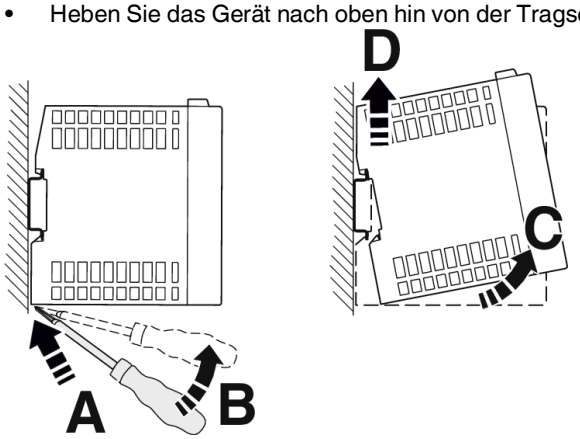


Bild 3-2 Demontage des Geräts

3.2 Versorgungsspannung anschließen

ACHTUNG: Elektrische Spannung
Das Gerät ist ausschließlich für den Betrieb mit Sicherheitskleinspannung (SELV/PELV) nach EN/IEC 62368-1 ausgelegt. Das Gerät darf nur an Geräte angeschlossen werden, die die Bedingungen der EN/IEC 62368-1 erfüllen. Sehen Sie eine Überstromschutzeinrichtung (I ≤ 5 A) in der Installation vor.

Das Gerät wird mit einer 24-V-DC-Spannung betrieben.

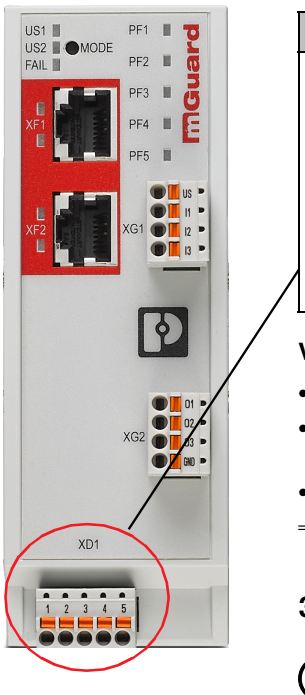
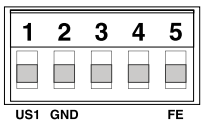


Tabelle 3-1 Spannungsversorgung über COMBICON-Steckverbindung

COMBICON	1	2	3	4	5
XD1	**US1**	**GND**	**nicht verfügbar**		**Funktionserde**
	18...36 V	0 V	**n. a.**	**n. a.**	FE

Versorgungsspannung anschließen

- Ziehen Sie die COMBICON-Steckverbindung **XD1** vom Gerät ab.
- Schließen Sie die Versorgungsspannung an die COMBICON-Steckverbindung an. Beachten Sie die Polarität (siehe Tabelle 3-1).
- Stecken Sie die COMBICON-Steckverbindung **XD1** auf das Gerät.

⇒ Sobald eine oder beide US-LEDs leuchten, ist das Gerät angeschlossen.

3.2.1 Das Gerät erden

ACHTUNG: Verletzungsgefahr durch Spannungsunfälle
Um Unfälle durch elektrische Spannungen zu vermeiden, muss eine vorschriftsmäßige und den Gegebenheiten angepasste Erdung des Geräts zwingend erfolgen.

Die Geräte müssen geerdet werden, damit mögliche Störungen vom Datentelegramm ferngehalten und auf Erdpotenzial abgeleitet werden können.

Gerät erden

- Montieren Sie das Modul auf einer geerdeten Tragschiene.
- Die Funktionserdung des Moduls erfolgt mit dem Aufrasten auf die geerdete Tragschiene oder über den **Klemmpunkt 5** (Funktionserde – FE) der COMBICON-Steckverbindung **XD1**.

3.3 Netzwerkverbindung anschließen

Das Netzwerk kann (geräteabhängig) über RJ45-Ports per Twisted-Pair-Kabel (IEEE 802.3i/u/ab) angeschlossen werden.

ACHTUNG: Fernmeldeanschlüsse
Schließen Sie die Netzwerkanschlüsse (Ethernet) des Geräts nur an LAN-Installationen an. Einige Fernmeldeanschlüsse verwenden ebenfalls RJ45-Anschlüsse, diese dürfen nicht mit den RJ45-Anschlüssen des Geräts verbunden werden.

Für den Betrieb mit 1000 Mbit/s (Gigabit) gilt: Die Verwendung von Leitungen mit vier Twisted-Pairs (acht Adern), die mindestens die Anforderungen nach CAT5e erfüllen, ist zwingend erforderlich.

3.3.1 Verwendung von RJ45-Ethernet-Steckern

Tabelle 3-2 Pin-Belegung der RJ45-Stecker

Pin-Nummer	10Base-T (10 Mbit/s)	100Base-TX (100 Mbit/s)	1000Base-T (1000 Mbit/s)
1	TD+ (Transmit)	TD+ (Transmit)	BI_DA+ (Bidirektional)
2	TD- (Transmit)	TD- (Transmit)	BI_DA- (Bidirektional)
3	RD+ (Receive)	RD+ (Receive)	BI_DB+ (Bidirektional)
4	–	–	BI_DB- (Bidirektional)
5	–	–	BI_DC+ (Bidirektional)
6	RD- (Receive)	RD- (Receive)	BI_DC- (Bidirektional)
7	–	–	BI_DD+ (Bidirektional)
8	–	–	BI_DD- (Bidirektional)

RJ45-Ethernet-Stecker anschließen

- Achten Sie auf die passende Kodierung des Steckers (siehe auch Tabelle 3-2).
- Verwenden Sie ausschließlich Twisted-Pair-Leitungen mit einer Impedanz von 100 Ω und einer Länge von maximal 100 m (pro Segment).
- Verwenden Sie ausschließlich geschirmte Twisted-Pair-Leitungen und passende abgeschirmte RJ45-Stecker. Stecken Sie die Ethernet-Leitung mit dem RJ45-Stecker in einen Port der Twisted-Pair-Schnittstelle (Netzwerkinterface 1 oder 2), bis der Stecker hörbar verrastet.

3.4 Schalteingänge/Schaltausgänge (I/Os) anschließen

ACHTUNG: Externe Spannungsquelle
Schließen Sie die Spannungs- und Masseausgänge (**O1–3** und **GND**) nicht an eine externe Spannungsquelle an.

Die Anschlussleitungen für Ein- und Ausgänge dürfen maximal 30 Meter lang sein.

Zwischen die Servicekontakte **US** und **I** (**1–3**) kann ein Taster oder ein Ein-/Aus-Schalter (z. B. Schlüsselschalter) angeschlossen werden (siehe Tabelle 3-3).

Die Servicekontakte können für verschiedene Schalt- oder Signalisierungsaufgaben verwendet werden.

Die Schalteingänge können mit Signalen externer Geräte beschaltet werden, z. B. mit Signalen einer Maschinensteuerung (SPS). Achten Sie in diesem Fall auf ein gleiches Potenzial und die zugelassenen Spannungs- und Stromwerte.

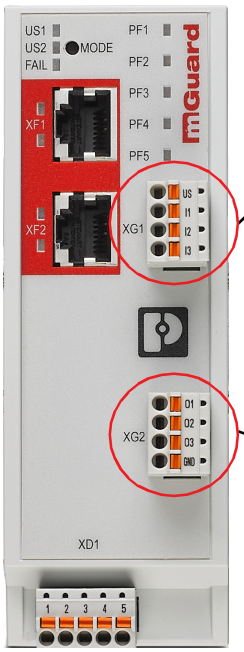


Tabelle 3-3 **Eingang I1–3**: Servicekontakte über COMBICON-Steckverbindung

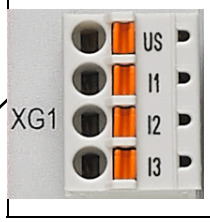
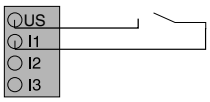
COMBICON XG1	Eingang (I1–3)		Beispiel
	**US**	Spannungsausgang (**US**) (+) (Kurzschlussfest)	
	I1	Schalteingänge **(I1–3)**	
	I2		
	I3		

Tabelle 3-4 **Ausgang O1–3**: Servicekontakte über COMBICON-Steckverbindung

COMBICON XG2	Ausgang (O1–3)		Beispiel
	**O1**	Schaltausgänge (**O1–3**)	
	O2	Kurzschlussfester Schaltausgang (24 V DC)	
	O3		
	GND	Masseanschluss (**GND**) (–) 0 V	

Die Schaltausgänge O1–3 sind potenzialbehaftet, dauerkurzschlussfest und für maximal 250 mA bei 18 ... 36 V DC ausgelegt.

I/Os anschließen

Die COMBICON-Steckverbindungen der Servicekontakte können während des Betriebs des Geräts entfernt oder aufgesetzt werden.

- Ziehen Sie die COMBICON-Steckverbindung **XG1** bzw. **XG2** vom Gerät ab.
- Schließen Sie die gewünschte Anschlussleitung an die COMBICON-Steckverbindung an (siehe Tabelle 3-3 und 3-4).
- Stecken Sie die COMBICON-Steckverbindung **XG1** bzw. **XG2** auf das Gerät.

3.5 SD-Karte verwenden

Beachten Sie, dass die Funktionalität der SD-Karte und des Produktes nur bei Einsatz einer Phoenix Contact SD-Karte (z. B. SD FLASH 2GB - 2988162) sichergestellt werden kann.

Beim Einsatz von SD-Karten anderer Anbieter wird empfohlen, die Kompatibilität der Karte vor der Verwendung sicherzustellen.

Der SD-Kartenhalter befindet sich auf der Rückseite des Geräts.

Technische Voraussetzung SD-Karte:

– SD- und SDHC-Karten bis max. 8 GB
– VFAT-kompatibles Dateisystem

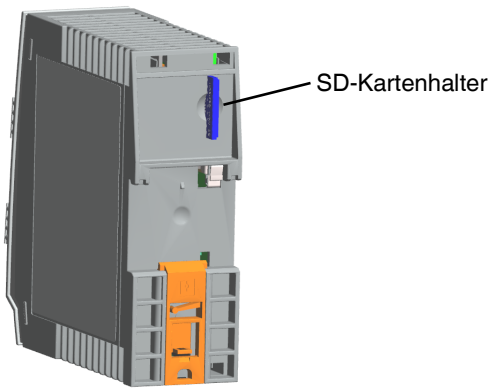


Bild 3-3 SD-Kartenhalter auf der Rückseite des Geräts

4 Erstinbetriebnahme

Die Erstinbetriebnahme des Geräts kann im *Easy Protect Mode* oder im *Router-Modus* erfolgen.

Easy Protect Mode (siehe Kapitel 4.2)

- Das Gerät wird unsichtbar in ein bestehendes Netzwerk eingefügt.
- Das Gerät muss und kann nicht konfiguriert werden.
- Die Firewall des Geräts schützt automatisch alle über Netzwerkinterface 2 (Netzzone 2 / XF2–XF5) angeschlossenen Geräte vor Netzwerkzugriffen über das Netzwerkinterface 1 (Netzzone 1 / XF1).
- Geschützte Geräte in der Netzzone 2 (XF2–XF5) können auf alle Geräte im Netzwerk zugreifen.

Router-Modus (siehe Kapitel 4.3)

- Das Gerät wird als Router/Gateway zwischen zwei Subnetzen betrieben.
- Die IP-Konfiguration des Geräts und der angeschlossenen Geräte muss an die eigenen Netzwerkstruktur angepasst werden.
- Alle Geräte der Netzzone 2 (XF2–XF5) können ihre IP-Konfiguration automatisch per DHCP vom Gerät erhalten.
- Die Firewall des Geräts schützt automatisch alle über Netzzone 2 angeschlossenen Geräte vor externen Netzwerkzugriffen aus Netzzone 1 (XF1).
- Erwünschte externe Zugriffe auf die geschützten Geräte können gezielt erlaubt werden (Firewall- und NAT-Regeln).
- Die geschützten Geräte in Netzzone 2 können auf alle Geräte in beiden Netzzonen zugreifen.
- Die geschützten Geräte in Netzzone 2 können auf Server-Dienste des Geräts zugreifen (WBM, DHCP, DNS, NTP).

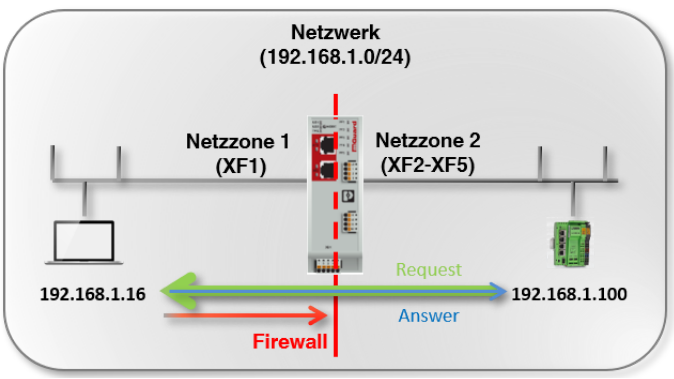
4.1 Erforderliche Komponenten

- Gerät mit COMBICON-Steckverbindung (für XD1)
- 24V-Stromversorgung
- Netzwerkkabel (Ethernet)
- Drahtbrücke (nur *Easy Protect Mode*)
- Konfigurationsrechner (nur *Router-Modus*)

4.2 Gerät im „Easy Protect Mode“ betreiben

Wird das Gerät im *Easy Protect Mode* betrieben, schützt es **automatisch** alle über Netzzone 2 (XF2–XF5) angeschlossenen Geräte vor externen Zugriffen (z. B. einzelne Maschinen oder über einen Switch angeschlossene Produktionszellen).

Das Gerät wird über seine Netzzonen 1 und 2 (XF1 und XF2–XF5) in das bestehende Netzwerk eingefügt, ohne dass die bestehende Netzwerkkonfiguration der angeschlossenen Geräte geändert werden muss (siehe Bild 4-1).



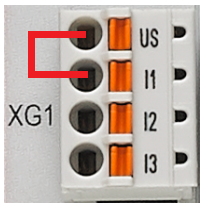


Bild 4-1 Gerät im *Easy Protect Mode* betreiben (Beispielkonfiguration)

Netzwerkverbindungen, die von den geschützten Geräten (aus Netzzone 2) aufgebaut werden, werden von der Firewall nicht blockiert.

Das Gerät selbst besitzt keine eigenen IP-Adressen und wird im Netzwerk nicht als Netzwerkteilnehmer erkannt.

Eine Konfiguration des Geräts ist grundsätzlich nicht notwendig und aufgrund der fehlenden Zugriffsmöglichkeit über das Web-based Management (HTTPS) auch nicht möglich.

Im *Easy Protect Mode* können Firmware-Updates über die Smart-Mode-Funktion „Update von SD-Karte“ durchgeführt werden (siehe Kapitel 5.1.4).

Verwenden Sie die jeweils aktuelle Firmware-Version

Da mit jeder neuen Firmware-Version sicherheitsrelevante Verbesserungen in das Produkt eingefügt werden, sollte grundsätzlich immer auf die neueste Firmware-Version aktualisiert werden.

Phoenix Contact stellt regelmäßig Firmware-Updates zur Verfügung. Diese finden Sie auf der Produktseite des jeweiligen Geräts (z. B. phoenixcontact.net/product/1153079).

- Stellen Sie sicher, dass die Firmware aller verwendeten Geräte immer auf dem aktuellen Stand ist.
- Beachten Sie die Change Notes / Release Notes zur jeweiligen Firmware-Version.
- Beachten Sie die Webseite des Product Security Incident Response Teams (PSIRT) von Phoenix Contact für Sicherheitshinweise zu veröffentlichten Sicherheitslücken.

4.2.1 Easy Protect Mode aktivieren

Um das Gerät im *Easy Protect Mode* zu betreiben, gehen Sie wie folgt vor:

- Trennen Sie das Gerät von der Spannungsversorgung.
- Überbrücken Sie die Servicekontakte **US** und **I1** des Geräts (COMBICON-Steckverbindung **XG1**) mit einer Kabelbrücke (siehe Bild 4-1 und Kapitel 3.4).
- Verbinden Sie das Gerät mit der Spannungsversorgung (siehe Kapitel 3.2, „Versorgungsspannung anschließen“).

⇒ Das Gerät wird im aktivierten *Easy Protect Mode* gestartet und betrieben.

4.2.2 Netzwerk-Clients schützen

- Verbinden Sie die zu schützenden Geräte über einen Netzwerkport (**XF2–XF5**) mit **Netzzone 2** des Geräts.

  (Um mehrere Geräte zu schützen, verbinden Sie diese über einen zusätzlichen Switch mit dem Gerät.)
- Verbinden Sie das umgebende Netzwerk über einen Switch mit **Netzzone 1 (XF1)**.

⇒ Alle Netzwerkpakete XF1 --> (XF2–XF5) werden verworfen.

⇒ Alle Netzwerkpakete (XF2–XF5) --> XF1 werden angenommen und weitergeleitet.

4.3 Gerät im „Router-Modus“ betreiben

Wird das Gerät im Router-Modus betrieben, arbeitet es als Gateway zwischen verschiedenen Subnetzen (siehe Bild 4-2).

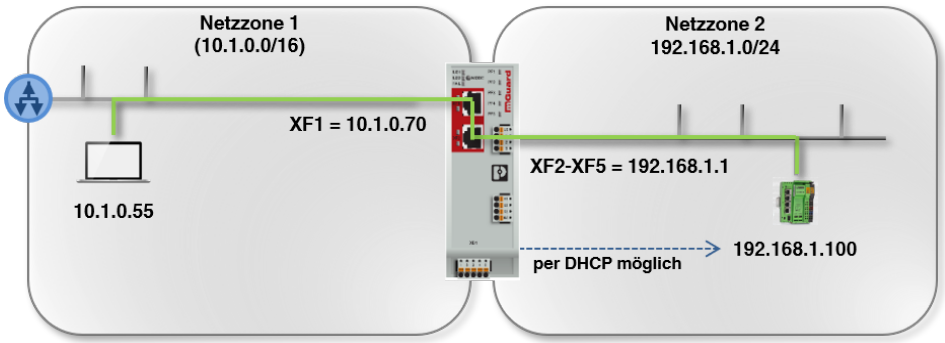


Bild 4-2 Gerät im Router-Modus betreiben (Beispielkonfiguration)

Der Datenverkehr wird zwischen den beiden Netzwerkinterfaces (Netzzonen) des Geräts weitergeleitet (*geroutet*).

In den Werkseinstellungen wird dabei der Datenverkehr von Netzzone 1 nach Netzzone 2 durch die Firewall blockiert.

Grundsätzlich können Clients einer Netzzone jedoch untereinander sowie mit Clients der andern Netzzone kommunizieren und Daten austauschen:

– Mithilfe der Firewall-Funktionen kann der Netzwerkzugriff auf einzelne oder mehrere Netzwerk-Clients gezielt erlaubt oder blockiert werden.
– Mithilfe der NAT-Funktionen kann der Datenaustausch zwischen den Netzzonen ermöglicht werden.

4.3.1 Gerät starten

Um das Gerät zu starten, gehen Sie wie folgt vor:

• Verbinden Sie das Gerät mit einer externen Spannungsversorgung (siehe Kapitel 3.2, „Versorgungsspannung anschließen“).

⇒ Das Gerät wird gestartet.

⇒ Die LED FAIL leuchtet kurz rot.

⇒ Während des Bootvorgangs leuchten die LEDs PF1–5 orange.

⇒ Die Betriebsbereitschaft des Geräts wird erreicht, wenn die LED PF1 grün blinkt (Herzschlag).

4.3.2 Netzwerkverbindung zum Gerät herstellen

Die im folgenden Beispiel verwendeten IP-Konfigurationen sind frei gewählt. Passen Sie die IP-Konfiguration an Ihre Netzwerkumgebung an, um Adresskonflikte zu vermeiden.

Um das Gerät mithilfe eines Webbrowsers zu konfigurieren (Web-based Management), müssen Sie es zunächst mit einen Konfigurationsrechner verbinden (siehe Bild 4-3).

Im Folgenden wird die Konfiguration des Geräts über Netzzone 2 (XF2–XF5) beschrieben. (Die Konfiguration über Netzzone 1 ist in den Werkseinstellungen nicht möglich.)

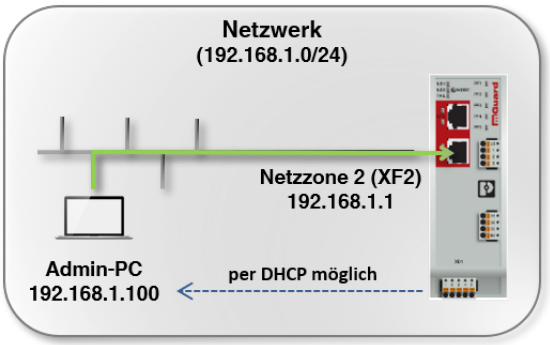


Bild 4-3 Netzwerkverbindung zum Gerät herstellen

Voraussetzung

Das Gerät und der Konfigurationsrechner (Admin-PC) müssen sich im gleichen Subnetz befinden. Eine beispielhafte Netzwerkkonfiguration ist in Tabelle 4-1 angegeben.

Tabelle 4-1 IP-Konfiguration (Beispiel): Netzwerkverbindung herstellen

Gerät	IP	Netzmaske	Gateway
Gerät (Werkseinstellung für XF2-XF5)	192.168.1.1	24 (255.255.255.0)	-
Konfigurationsrechner (Per **DHCP** vom Gerät zugewiesen oder **statisch** konfiguriert.)	192.168.1.100	24 (255.255.255.0)	192.168.1.1

Vorgehen

- Verbinden Sie den Konfigurationsrechner direkt oder über das Netzwerk mit einem Netzwerkport XF2–XF5 der Netzzone 2 des Geräts (siehe Bild 4-3).
- Die IP-Einstellung des Konfigurationsrechners kann automatisch per DHCP zugewiesen oder statisch konfiguriert werden (siehe unten).

⇒ Wenn der Konfigurationsrechner bereits so konfiguriert ist, dass er seine IP-Einstellung per DHCP bezieht, weist ihm das Gerät in **den Werkseinstellungen** über Netzzone 2 (XF2–XF5) automatisch eine IP-Konfiguration zu (z. B. 192.168.1.100/24).

IP-Konfiguration prüfen

- Öffnen Sie das Windows-Startmenü und tippen Sie *„cmd“,* um eine Kommandozeile zu öffnen.
- Geben Sie den Befehl „*ipconfig*“ ein und drücken Sie die Eingabetaste.

⇒ *IPv4-Adresse*, *Subnetzmaske* und *Standard-Gateway* des Ethernet-Adapters werden angezeigt.

IP-Einstellung per DHCP beziehen

Um die IP-Einstellung des Konfigurationsrechners automatisch zu beziehen, gehen Sie wie folgt vor:

- Öffnen Sie das Windows-Startmenü und tippen Sie *„Systemsteuerung“*.
- Öffnen Sie (*Netzwerk und Internet*) / *Netzwerk- und Freigabecenter*
- Klicken Sie auf *„Adaptereinstellungen ändern“.*
- Klicken Sie mit der rechten Maustaste auf den gewünschten Netzwerkadapter und wählen Sie den Menübefehl „*Eigenschaften*“.
- Doppelklicken Sie auf das Element „*Internetprotokoll, Version 4 (TCP/IPv4)*“.

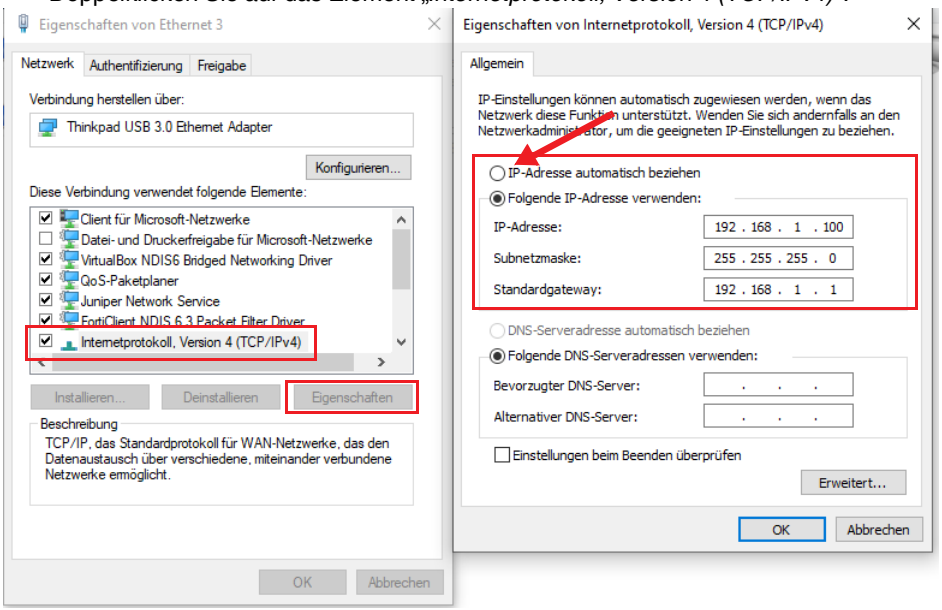


Bild 4-4 IP-Einstellung des Konfigurationsrechners (Admin-PC) ändern

- Wählen Sie „*IP-Adresse automatisch beziehen*“.
- Bestätigen Sie mit „*OK*“

⇒ Das Gerät weist dem Konfigurationsrechner eine IP-Adresse aus dem Subnetz 192.168.1.0/24 zu (z. B. 192.168.1.100).

⇒ Das Gerät dient dem Konfigurationsrechner als Standard-Gateway.

Statische IP-Einstellung manuell eintragen

Um die IP-Einstellungen des Konfigurationsrechners (Windows) statisch zu konfigurieren, gehen Sie wie folgt vor:

- Öffnen Sie das Windows-Startmenü und tippen Sie *„Systemsteuerung“*.
- Gehen Sie vor wie oben beschrieben.
- Wählen Sie „*Folgende IP-Adresse verwenden*“.
  - Geben Sie die Werte entsprechend dem Beispiel in Bild 4-4 / Tabelle 4-1 ein.
- Bestätigen Sie mit „*OK*“

⇒ Sie haben dem Konfigurationsrechner eine IP-Adresse aus dem Subnetz 192.168.1.0/24 zugewiesen.

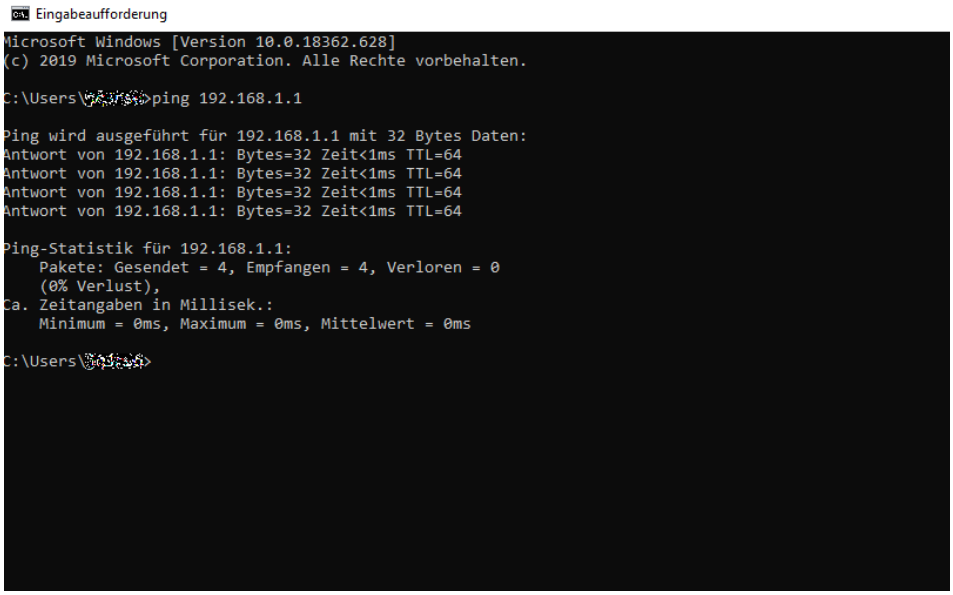
⇒ Das Gerät dient dem Konfigurationsrechner als Standard-Gateway.

Verbindung testen

Um zu testen, ob der Konfigurationsrechner das Gerät über das Netzwerk erreichen kann, gehen Sie wie folgt vor:

- Öffnen Sie das Windows-Startmenü und tippen Sie *„cmd“,* um eine Kommandozeile zu öffnen.
- Geben Sie den Befehl „*ping 192.168.1.1*“ ein und drücken Sie die Eingabetaste.

⇒ Aus der Antwort der Ping-Anfrage können Sie erkennen, ob das Gerät auf Anfragen des Konfigurationsrechners reagiert.



4.4 Gerät mit einer gespeicherten Konfiguration von SD-Karte in Betrieb nehmen

Mithilfe der Funktion „External configuration storage (ECS)“ ist es möglich, die aktuelle Gerätekonfiguration auf einer SD-Karte zu speichern (siehe Anwenderhandbuch „UM DE MGUARD NT“, erhältlich unter phoenixcontact.net/product/1153079).

Eine auf SD-Karte gespeicherte Konfiguration kann in ein neues Gerät importiert werden.

Damit ist es möglich, einen Gerätetausch schnell und unkompliziert durchzuführen, sollte es bei einem Gerät einmal zu einer Fehlfunktion kommen.

Des Weiteren können neue Geräte leicht auf der Basis einer bestehenden Konfiguration in Betrieb genommen werden.

Voraussetzung: Firmware-Version „SD-Karte“ ist kleiner/gleich Firmware-Version „Gerät“.

Gehen Sie wie folgt vor:

- Verwenden Sie ein fabrikneues Gerät oder ein Gerät, bei dem die Werkseinstellungen mittels Smart-Mode (siehe Kapitel 5.1.3) wiederhergestellt wurden.
- Setzen Sie die SD-Karte mit der gespeicherten Konfiguration in den SD-Kartenhalter ein. Die drei Dateien *users_pass.json, snmp-pass.conf* und *configuration.json* müssen auf der SD-Karte vorhanden sein (einzeln oder in gepackter Form als *mGuard.tar.gz:* Die Einzeldateien werden prioritär verwendet!).
- Starten Sie das Gerät.

⇒ Die Konfiguration wird von der SD-Karte automatisch in das Gerät importiert und dort angewendet.

⇒ Im Falle eines Fehlers leuchten die LEDs FAIL und PF1 rot.

4.5 Web-based Management verwenden

4.5.1 Unterstützte Webbrowser

Unterstützt werden folgende Webbrowser in ihrer jeweils aktuellen Version:

– *Mozilla Firefox, Google Chrome, Microsoft Edge*

4.5.2 Unterstützte Benutzer

Nur der Benutzer *admin* kann sich auf dem Gerät anmelden.

Der Benutzer *admin* hat einen funktional uneingeschränkten Zugriff auf das Web-based Management (WBM) und die RESTful Configuration API (*Config API*) des Geräts.

4.5.3 Beim Gerät anmelden

Um sich beim WBM des Geräts anzumelden, gehen Sie wie folgt vor:

- Verbinden Sie den Konfigurationsrechner mit dem Gerät (siehe Kapitel 4.3.2).
- Starten Sie einen Webbrowser auf dem Konfigurationsrechner.
- Geben Sie die IP-Adresse des angeschlossenen Netzwerkinterfaces des Geräts in die Adresszeile des Webbrowsers ein (z. B. **https**://192.168.1.1).

⇒ Da das Gerät von Phoenix Contact mit einem selbst-signierten Sicherheitszertifikat ausgestattet wurde, das Ihrem Webbrowser nicht bekannt ist, erscheint eine Zertifikats-Warnung.

Bild 4-5 Zertifikatswarnung (Firefox)

- Bestätigen Sie, dass Sie trotz der Warnung fortfahren möchten, indem Sie eine Ausnahme hinzufügen, um die vermeintlich „*unsichere*“ Webseite zu öffnen.
- Klicken Sie dazu in Firefox beispielsweise auf:
  Erweitert >> *Ausnahme hinzufügen...* >> *Sicherheits-Ausnahmeregel bestätigen*
- Gehen Sie bei anderen Webbrowsern analog vor.

⇒ Die Anmeldeseite des Web-based Managements wird geöffnet.

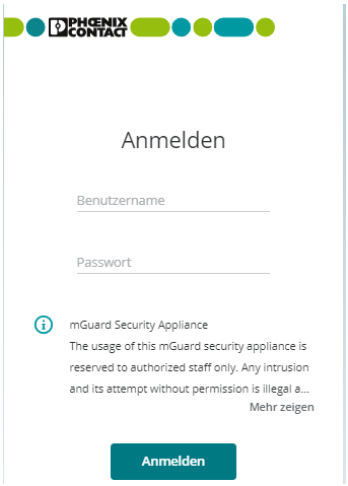


Bild 4-6 Anmeldeseite des Web-based Managements

- Melden Sie sich mit dem Benutzernamen *admin* und dem zugehörigen Administrator-Passwort (Werkseinstellungen: *private*) an.

⇒ Die Startseite des Web-based Managements von mGuardNT wird geöffnet.

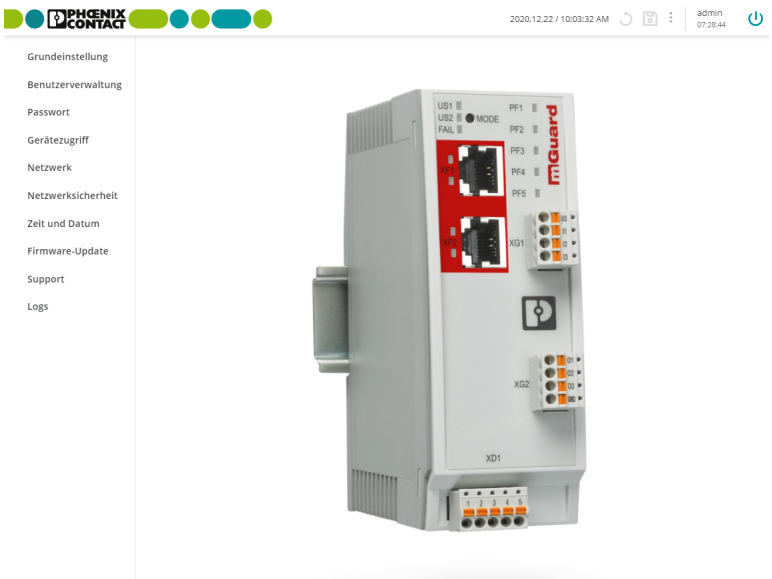


Bild 4-7 Startseite des Web-based Managements

Die Funktionen, die mittels Web-based Management konfiguriert werden können, werden im Anwenderhandbuch „*FL MGUARD 1000 – Web-based Managemen*t“ (UM DE MGUARD NT) beschrieben.

Erhältlich im Download-Bereich der entsprechenden Produktseite im Phoenix Contact Web-Shop, z. B. unter phoenixcontact.net/product/1153079.

4.6 Gerät neu starten (Reboot)

ACHTUNG: Alle nicht gespeicherten Änderungen gehen verloren.

Um ein betriebsbereites Gerät neu zu starten (*Reboot*), gehen Sie wie folgt vor:

– Möglichkeit 1: Drücken Sie die Mode-Taste (5 Sekunden)
– Möglichkeit 2: Unterbrechen Sie die kurzzeitig die Spannungsversorgung
– Möglichkeit 3: Starten Sie das Gerät über das WBM neu (siehe Anwenderhandbuch „UM DE MGUARD NT“, erhältlich unter phoenixcontact.net/product/1153079)

Drücken der Mode-Taste

• Drücken Sie die Mode-Taste mindestens 5 Sekunden.
⇒ Die LED FAIL leuchtet rot.
• Lassen Sie die Mode-Taste los.
⇒ Das Gerät wird neu gestartet.
⇒ Die LEDs PF1–5 leuchten orange.
⇒ Die Betriebsbereitschaft des Geräts wird erreicht, wenn die LED PF1 grün blinkt (Herzschlag).

Unterbrechen der Spannungsversorgung

• Unterbrechen Sie kurzzeitig die Spannungsversorgung des Geräts.
⇒ Das Gerät wird neu gestartet.
⇒ Die LEDs PF1–5 leuchten orange.
⇒ Die Betriebsbereitschaft des Geräts wird erreicht, wenn die LED PF1 grün blinkt (Herzschlag).

Via Web-based Management

• Öffnen Sie das Menü: **Verwaltung >> System**
• Klicken Sie auf die Schaltfläche **Neustart**, um das Gerät neu zu starten.

4.7 RESTful Configuration API verwenden

Die Verwendung der *Config API* wird im Anwenderhandbuch „*FL MGUARD 1000 – RESTful Configuration API*“ (UM DE MGUARD NT CONFIG API) beschrieben. Erhältlich im Download-Bereich der entsprechenden Produktseite im Phoenix Contact Web-Shop, z. B. unter phoenixcontact.net/product/1153079.

Nur für erfahrene Anwender

Neben der Konfiguration über das Web-based Management, kann das Gerät auch über die RESTful Configuration API (kurz: *Config API*) konfiguriert werden.

Die *Config API* wird über einen RESTful-Webserver des Geräts bereitgestellt.

Die Übertragung der Daten erfolgt über das HTTP(S)-Protokoll, das auch zum Abrufen von Webseiten verwendet wird.

5 Smart-Mode

Über den Smart-Mode können Sie Gerätefunktionen aufrufen, ohne Zugriff auf ein Management-Interface des Geräts zu haben. Vier Smart-Mode-Funktionen stehen zur Verfügung:

– „Verlassen ohne Änderung (PF1)“
– „Wiederherstellen des Konfigurationszugriffs (PF2)“
– „Wiederherstellen der Werkseinstellungen (PF3)“
– „Update von SD-Karte (PF4)“

Die Smart-Mode-Funktion „PF5“ ist ausschließlich für Wartungszwecke und die Verwendung durch den Hersteller reserviert. Eine falsche Verwendung kann zu einer unwiderruflichen Löschung der Gerätekonfiguration führen.

5.1 Verfügbare Smart-Mode-Funktionen

5.1.1 Verlassen ohne Änderung (PF1)

Anwendungsfall

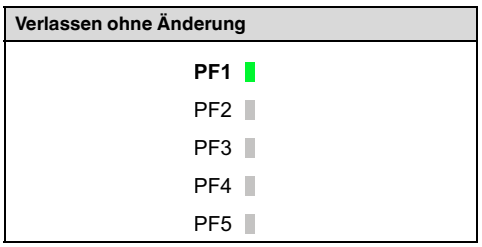
Der Smart-Mode soll verlassen werden, ohne dass Änderungen vorgenommen werden.

Ergebnis

– Das Gerät wird neu gestartet und bootet die aktuell installierte Firmware mit der zuletzt gespeicherten Konfiguration.
– Alle Einstellungen, Passwörter und Zertifikate bleiben erhalten.

Ausführung

⇒ siehe „Smart-Mode verwenden“ auf Seite 47



5.1.2 Wiederherstellen des Konfigurationszugriffs (PF2)

Anwendungsfälle

– Die IP-Konfiguration des Geräts ist nicht bekannt. Es ist deshalb nicht mehr möglich, auf das Web-based Management oder die *Config API* des Geräts zuzugreifen.
– Die IP-Konfiguration von Netzzone 2 (XF2–XF5) soll auf die Werkseinstellungen zurückgesetzt werden.

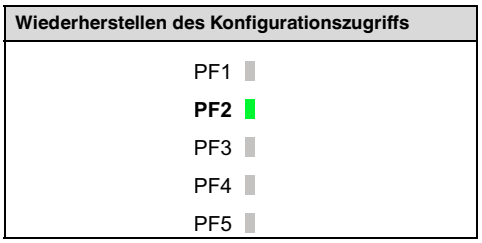
Ergebnis

Der Zugriff auf das Gerät über die werkseitig voreingestellte IP-Adresse ist wieder möglich:

– Die werkseitig voreingestellte Netzwerkkonfiguration von Netzzone 2 (XF2–XF5) wird wiederhergestellt: Modus: Router, IP-Adresse: 192.168.1.1, Netzmaske: 24
– Die werkseitig voreingestellte Zugriffsregel für den Webserver (WBM) wird für Netzzone 2 wiederhergestellt (siehe Kapitel 2.6).
– Die übrige Gerätekonfiguration, Benutzer, Passwörter und Zertifikate bleiben erhalten.

Ausführung

⇒ siehe „Smart-Mode verwenden“ auf Seite 47



5.1.3 Wiederherstellen der Werkseinstellungen (PF3)

Anwendungsfälle

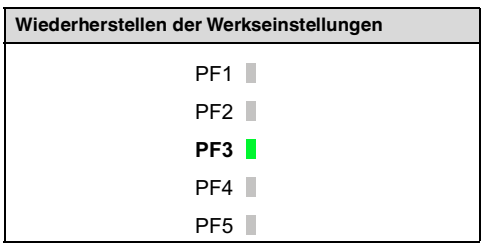
– Das Administrator-Passwort und andere Passwörter sind nicht bekannt. Es ist deshalb nicht mehr möglich, sich auf dem Gerät anzumelden.
– Die Gerätekonfiguration, Benutzer, Passwörter und Zertifikate sollen sicher und unwiderruflich gelöscht werden.
– Das Gerät soll außer Betrieb genommen werden.

Ergebnis

– Die aktuelle Gerätekonfiguration, Benutzer, Passwörter und Zertifikate werden sicher und unwiderruflich gelöscht.
– Das Gerät wird mit den Werkseinstellungen neu konfiguriert.

Ausführung

⇒ siehe „Smart-Mode verwenden“ auf Seite 47



5.1.4 Update von SD-Karte (PF4)

Wenn das via Smart-Mode ausgeführte Update fehlschlägt, versuchen Sie bitte stattdessen, das Gerät über das Web-based Management zu aktualisieren. Schlägt das Update dabei weiterhin fehl, beachten Sie bitte die in der Benutzeroberfläche angezeigten Fehlermeldungen oder die Log-Dateien, um das Problem zu lösen.

Weitere Hinweise zu Firmware-Updates finden Sie im Anwenderhandbuch „UM DE MGUARD NT“, erhältlich unter phoenixcontact.net/product/1153079.

Anwendungsfall

– Das Gerät soll von SD-Karte auf eine höhere Firmware-Version upgedatet werden, ohne dass ein Zugriff auf ein Management-Interface besteht.

  Die Gerätekonfiguration, Passwörter und Zertifikate sollen erhalten bleiben.

Ergebnis

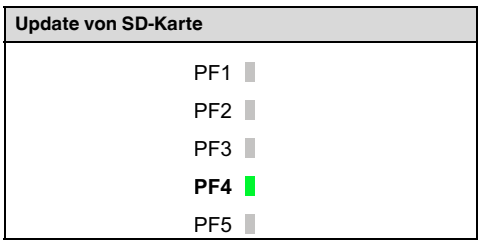
– Die Update-Datei auf der SD-Karte wird für ein Firmware-Update verwendet.
– Die Gerätekonfiguration, Passwörter und Zertifikate bleiben erhalten.

Voraussetzung

– **Eine** gültige Update-Datei befindet sich auf der ersten Partition der SD-Karte.
– **Achtung**: Sind mehr als eine Update-Datei auf der SD-Karte vorhanden, führt dies zu einem Abbruch: die LEDs PF1–5 leuchten rot.
– Ein „Update“ zur gleichen oder ein Downgrade von einer höheren auf eine niedrigere Firmware-Version ist nicht möglich und führt zu einem Abbruch: die LEDs PF1–5 leuchten rot.

Ausführung

⇒ siehe „Smart-Mode verwenden“ auf Seite 47



5.2 Smart-Mode verwenden

Der Smart-Mode wird durch das Drücken der Mode-Taste nach dem Gerätestart aktiviert.

Drücken Sie die Mode-Taste erst, nachdem Sie das Gerät gestartet haben.
Wird die Mode-Taste bereits beim Starten des Geräts gedrückt gehalten, kann anschließend nicht mehr auf das Gerät zugegriffen werden. Starten Sie in diesem Fall das Gerät neu, indem Sie die Spannungsversorgung kurz unterbrechen.

5.2.1 Smart-Mode aktivieren

- Starten Sie das Gerät, indem Sie es an die Versorgungsspannung anschließen.
- Drücken Sie **innerhalb von zwei Sekunden** die Mode-Taste und halten Sie diese gedrückt.

⇒ Nach ca. 5 Sekunden blinken alle PF-LEDs (PF1–5) grün.

- Lassen Sie die Mode-Taste los.

⇒ Die ausgewählte Smart-Mode-Funktion wird durch die zugehörige PF-LED (grün) angezeigt (siehe Tabelle 5-1).

⇒ Zusätzlich blinken alle PF-LEDs alle vier Sekunden dreimal grün.

⇒ Nach der Aktivierung ist die Funktion „Verlassen ohne Änderung“ (PF1) ausgewählt.

5.2.2 Smart-Mode-Funktion auswählen

- Drücken Sie kurz die Mode-Taste, um die jeweils nächste Funktion auszuwählen.

⇒ Die ausgewählte Funktion wird durch die zugehörige PF-LED angezeigt (siehe unten).

Tabelle 5-1 Smart-Mode-Funktionen im Status „Ausgewählt“

Verlassen ohne Änderung	Wiederherstellen des Konfigurationszugriffs	Wiederherstellen der Werkseinstellungen	Update von SD-Karte
PF1	PF1	PF1	PF1
PF2	**PF2**	PF2	PF2
PF3	PF3	**PF3**	PF3
PF4	PF4	PF4	**PF4**
PF5	PF5	PF5	PF5
Zusätzlich blinken alle PF-LEDs alle vier Sekunden simultan dreimal grün.			

5.2.3 Smart-Mode-Funktion ausführen

- Um die **ausgewählte** Funktion auszuführen, gehen Sie wie folgt vor:
  - Drücken Sie die Mode-Taste und halten Sie diese gedrückt.
  - ⇒ Nach ca. 5 Sekunden blinken alle PF-LEDs grün (schnell).
  - Lassen Sie die Mode-Taste los.

⇒ Die **ausgewählte** Funktion wird ausgeführt.

⇒ Alle nicht der Funktion zugehörigen PF-LEDs leuchten orange (siehe Tabelle 5-2).

ACHTUNG: Unterbrechen Sie nicht die Stromversorgung zum Gerät!
Eine Unterbrechung der Stromversorgung kann zu einem Gerätedefekt führen.

⇒ Wenn alle PF-LEDs grün leuchten, wurde die Funktion erfolgreich ausgeführt.

- Starten Sie das Gerät neu.

5.2.4 Smart-Mode verlassen

Der Smart-Mode kann nur verlassen werden, indem eine Smart-Mode-Funktion ausgewählt und angewendet wird:

- Smart-Mode-Funktion PF1: Der Smart-Mode wird verlassen, ohne dass Änderungen vorgenommen werden. Das Gerät wird neu gestartet.
- Smart-Mode-Funktionen PF2–4: Die ausgewählte Smart-Mode-Funktion wird ausgeführt. Nach erfolgreichem Abschluss der Smart-Mode-Funktion muss das Gerät neu gestartet werden.

5.2.5 LED-Anzeige (Smart-Mode)

Beispiel „Wiederherstellen der Werkseinstellungen“

Tabelle 5-2 LED-Anzeige: Smart-Mode „Wiederherstellen der Werkseinstellungen“

Ausgewählt	Wird ausgeführt	Erfolgreich beendet	Fehlgeschlagen
PF1 PF2 **PF3** PF4 PF5	PF1 PF2 PF3 PF4 PF5	PF1 PF2 PF3 PF4 PF5	PF1 PF2 PF3 PF4 PF5
Die LED zeigt an, welche Smart-Mode-Funktion ausgewählt wurde (siehe Tabelle 5-1). Zusätzlich blinken PF1–5 alle vier Sekunden simultan dreimal grün.	Die Smart-Mode-Funktion wird ausgeführt: Die Firmware wird auf das Gerät geschrieben. **ACHTUNG: Eine Unterbrechung der Stromversorgung kann das Gerät beschädigen!** **Schalten Sie das Gerät nicht aus!** Warten Sie, bis die Funktion erfolgreich ausgeführt wurde.	Die Smart-Mode-Funktion wurde erfolgreich ausgeführt. Starten Sie das Gerät neu.	Starten Sie im Fehlerfall das Gerät neu und wenden Sie sich im weiteren Fehlerfall an Ihren Support. Ein schwerwiegender Fehler kann auch durch die LED „FAIL“ angezeigt werden.

6 Gerätetausch, Gerätedefekt und Reparatur

6.1 Sicheres löschen von sensitiven Daten

ACHTUNG: Schützen Sie sensitive Daten vor unbefugten Dritten
Damit keine geschützten Daten bei der Außerbetriebnahme auf dem Gerät verbleiben und von unbefugten Dritten eingesehen werden können, müssen die Daten sicher und unwiderruflich gelöscht werden.

Führen Sie den Smart-Mode „Wiederherstellen der Werkseinstellungen (PF3)“ aus, um Daten auf dem Gerät sicher und unwiderruflich zu löschen (siehe Kapitel 5.1.3).

6.2 Gerätetausch

ACHTUNG: Gerätebeschädigung
Montieren und demontieren Sie die Geräte nur im spannungsfreien Zustand!

Gehen Sie bei einem Gerätetausch wie folgt vor:

- Schalten Sie das Gerät spannungsfrei.
- Entfernen Sie alle Leitungen.
- Entnehmen Sie die SD-Karte.
- Demontieren Sie das Gerät wie in Kapitel 3.1 beschrieben.
- Tauschen Sie das Gerät gegen ein identisches Gerät (gleiche Artikelnummer), fabrikneu oder mit Werkseinstellungen (siehe Kapitel 5.1.3), aus.
- (Optional): Stellen Sie eine gespeicherte Konfiguration des alten Geräts auf dem neuen Gerät wieder her (siehe Kapitel 6.2.1).

6.2.1 Wiederherstellen einer gespeicherten Konfiguration mittels SD-Karte (ECS)

Eine genaue Beschreibung finden Sie im Anwenderhandbuch „UM DE MGUARD NT“, erhältlich unter phoenixcontact.net/product/1153079.

Für alle **neuen Geräte** oder Geräte, die mittels Smart-Mode (siehe Kapitel 5.1.3) auf Werkseinstellungen zurückgesetzt wurden, gilt:

Eine auf der eingesetzten SD-Karte gespeicherte Konfiguration/Benutzerverwaltung wird beim Start bzw. der Inbetriebnahme des Geräts automatisch in das Gerät importiert und dort angewendet.

Voraussetzung:

– Die gespeicherte Konfiguration ist auf der SD-Karte enthalten: einzeln (*users_pass.json, snmp-pass.conf* und *configuration.json*) oder in gepackter Form (*mGuard.tar.gz*). Die Einzeldateien werden prioritär verwendet!
– Firmware-Version „SD-Karte“ ist kleiner/gleich Firmware-Version „Gerät“.
– Tritt während des Imports ein Fehler auf, startet das Gerät in den Werkseinstellungen. Die LEDs FAIL und PF1 leuchten zusätzlich rot.

6.3 Gerätedefekt und Reparatur

Reparaturen dürfen ausschließlich von Phoenix Contact vorgenommen werden.

- Senden Sie defekte Geräte zur Reparatur oder zum Erhalt eines Ersatzgeräts an Phoenix Contact zurück.
- Verwenden Sie bei Rücksendung vorzugsweise die Originalverpackung.
- Legen Sie der Rücksendung einen Vermerk bei, dass es sich um eine Retoure handelt.
- Legen Sie der Rücksendung eine Fehlerbeschreibung bei.
- Beachten Sie die folgenden Hinweise, falls die Originalverpackung nicht mehr vorliegt:
  - Beachten Sie beim Transport die Angaben zur Luftfeuchtigkeit und zum Temperaturbereich (siehe Kapitel 7).
  - Verwenden Sie ggf. Entfeuchtungsmittel.
  - Schützen Sie elektrostatisch gefährdete Bauteile durch eine entsprechende ESD-Verpackung.
  - Wählen Sie die Verpackung in ausreichender Größe und Materialstärke.
  - Verwenden Sie als Füllmaterial ausschließlich Luftpolsterfolien.
  - Versehen Sie die Transportverpackung gut sichtbar mit Warnhinweisen.
  - Achten Sie darauf, dass bei Inlandspaketen der Lieferschein im Paket verstaut wird und bei Auslandspaketen der Lieferschein in einer Lieferscheintasche außen gut sichtbar angebracht wird.

6.4 Entsorgung

Die durchgestrichene Mülltonne weist darauf hin, dass Sie den Artikel getrennt sammeln und entsorgen müssen. Phoenix Contact oder unsere Servicepartner nehmen den Artikel zur kostenlosen Entsorgung zurück. Informationen zu den angebotenen Entsorgungsmöglichkeiten finden Sie unter www.phoenixcontact.com.

Entsorgen Sie nicht mehr benötigte Verpackungsmaterialien (Kartonage, Papier, Luftpolsterfolie etc.) im Hausmüll gemäß den jeweils gültigen nationalen Vorschriften.

7 Technische Daten

7.1 FL MGUARD 1102/1105

Tabelle 7-1 Technische Daten

Allgemeine Daten (FL MGUARD 1102 / FL MGUARD 1105)	
Plattform	Marvell Armada 3720
Netzwerk-Schnittstellen	
FL MGUARD 1102	2 Ethernet-Schnittstellen mit: – RJ45 | Full Duplex | Auto-MDIX – Ethernet (10Base-T / IEEE 802.3i) – Fast Ethernet (100Base-TX / IEEE 802.3u) – Gigabit Ethernet (1000Base-T / IEEE 802.3ab)
FL MGUARD 1105	5 Ethernet-Schnittstellen mit: – RJ45 | Full Duplex | Auto-MDIX – Ethernet (10Base-T / IEEE 802.3i) – Fast Ethernet (100Base-TX / IEEE 802.3u) – Gigabit Ethernet (1000Base-T / IEEE 802.3ab)
Digitale Ein- und Ausgänge	Je 3 digitale Ein- und Ausgänge
Diagnose-Werkzeuge	Status- und Diagnose-LEDs | Digitale I/Os | Log-Dateien
Besonderheiten	Echtzeituhr | Trusted Platform Module (TPM) | Temperatursensor
Umgebungstemperatur (Betrieb)	0 °C ... +60 °C
Umgebungstemperatur (Lagerung/Transport)	-40 °C ... +70 °C
Zulässige Luftfeuchtigkeit (Betrieb)	10 % ... 95 % (keine Betauung)
Schutzart	IP20
Schutzklasse	Class 3 VDE 0106; IEC 60536, nur für den Innenbereich
Luftdruck (Betrieb)	68 kPa ... 108 kPa, 3000 m ü.N.N.
Umgebungsverträglichkeit	Frei von lackbenetzungsstörenden Stoffen nach VW-Spezifikation
Verschmutzungsgrad	2
Überspannungskategorie	Keine
Einbaulage	Senkrecht auf einer Normtragschiene
Verbindung zur Schutzerde	Durch Aufrasten auf eine geerdete Tragschiene oder über den Klemmpunkt 5 der COMBICON-Steckverbindung XD1
Gehäusemaße (Breite x Höhe x Tiefe) in mm	45 x 130 x 130 (Tiefe ab Oberkante Hutschiene)
Gewicht (exklusive Verpackung) Gewicht (inklusive Verpackung)	280 g 297 g

Firmware- und Leistungswerte	
Unterstützte Firmware	ab mGuardNT 1.3.2
Management-Support	Web-based Management | RESTful Configuration API | SD-Karte

Versorgungsspannung (US1)	
Anschluss	Über COMBICON-Steckverbindung (Push-in-Federanschluss); maximaler Leiterquerschnitt = 1,5 mm^2 (Kupferdrähte der Kategorie *75°C* oder gleichwertig verwenden)
Nennwert	24 V DC
Zulässiger Spannungsbereich	

Versorgungsspannung (US1)	
FL MGUARD 1102 FL MGUARD 1105	18 V DC ... 36 V DC
Zulässige Welligkeit (innerhalb des zulässigen Spannungsbereichs)	3,6 V_{PP}
Maximal Stromaufnahme (US = Min, T_{amb} = Max, DO_I = Max)	
FL MGUARD 1102	1,00 A
FL MGUARD 1105	1,06 A
Typische Stromaufnahme (US = Min, T_{amb} = Max, DO_I = Max)	
FL MGUARD 1102	0,12 A
FL MGUARD 1105	0,18 A
Prüfspannung	500 V DC für eine Minute

Netzwerkschnittstellen	
Eigenschaften der RJ45-Anschlüsse	
Anzahl	
FL MGUARD 1102	2
FL MGUARD 1105	5
Anschlussformat	8-polige RJ45-Buchse
Anschlussmedium	Twisted-Pair-Leitung mit einem Leiterquerschnitt von 0,14 mm^2 ... 0,22 mm^2
Leitungsimpedanz	100 Ohm
Übertragungsrate	10/100/1000 Mbit/s
Maximale Leitungslänge (Twisted-Pair)	100 m (pro Segment)

Digitale Aus- und Eingänge	
Digitale Ausgänge	
Anzahl	3
Spannung Ausgangssignal	18 V DC ... 36 V DC
Stromtragfähigkeit	250 mA
Digitale Eingänge	
Anzahl	3
Spannung Eingangssignal	0 V DC ... 36 V DC
Maximaler Eingangsstrom	3,5 mA

Mechanische Prüfungen	
Vibrationsfestigkeit nach IEC 60068-2-6	Betrieb/Lagerung/Transport: 5 g, 10 Hz ... 150 Hz
Freier Fall nach IEC 60068-2-32	1 m

Konformität zu EMV-Richtlinien	
Entwickelt nach IEC 61000-6-2	
Störaussendung nach EN 55016-2-1:2014 (leitungsgeführte Störaussendung)	Klasse B
Störaussendung nach EN 55016-2-3:2010 + A1:2010 + AC:2013 + A2:2014 (gestrahlte Störaussendung)	Klasse A

Konformität zu EMV-Richtlinien	
Störfestigkeit nach EN 61000-4-2 (IEC 1000-4-2) (ESD)	Anforderungen gem. DIN EN 61000-6-2
Kontaktentladung:	Prüfschärfegrad 3, Beurteilungskriterium B
Luftentladung:	Prüfschärfegrad 3, Beurteilungskriterium B
indirekte Entladung:	Prüfschärfegrad 3, Beurteilungskriterium B
Störfestigkeit nach EN 61000-4-3 (IEC1000-4-3) (elektromagnetische Felder)	Anforderungen gem. DIN EN 61000-6-2
	Prüfschärfegrad 3, Beurteilungskriterium A
Störfestigkeit nach EN 61000-4-6 (IEC1000-4-6) (leitungsgeführt)	Anforderungen gem. DIN EN 61000-6-2
	Prüfschärfegrad 3, Beurteilungskriterium A
Störfestigkeit nach EN 61000-4-4 (IEC1000-4-4) (Burst)	Anforderungen gem. DIN EN 61000-6-2
Datenleitungen:	Prüfschärfegrad 3, Beurteilungskriterium A
Spannungsversorgung:	Prüfschärfegrad 3, Beurteilungskriterium A
Servicekontakte:	Prüfschärfegrad 3, Beurteilungskriterium A
Störfestigkeit nach EN 61000-4-5 (IEC1000-4-5) (Surge)	Anforderungen gem. DIN EN 61000-6-2
Datenleitungen:	Prüfschärfegrad 2, Beurteilungskriterium B
Spannungsversorgung:	Prüfschärfegrad 1, Beurteilungskriterium B
Servicekontakte:	Prüfschärfegrad 1, Beurteilungskriterium B

Sonstiges	
Konformität	CE-konform

Bitte beachten Sie folgende Hinweise

Allgemeine Nutzungsbedingungen für Technische Dokumentation

Phoenix Contact behält sich das Recht vor, die technische Dokumentation und die in den technischen Dokumentationen beschriebenen Produkte jederzeit ohne Vorankündigung zu ändern, zu korrigieren und/oder zu verbessern, soweit dies dem Anwender zumutbar ist. Dies gilt ebenfalls für Änderungen, die dem technischen Fortschritt dienen.

Der Erhalt von technischer Dokumentation (insbesondere von Benutzerdokumentation) begründet keine weitergehende Informationspflicht von Phoenix Contact über etwaige Änderungen der Produkte und/oder technischer Dokumentation. Sie sind dafür eigenverantwortlich, die Eignung und den Einsatzzweck der Produkte in der konkreten Anwendung, insbesondere im Hinblick auf die Befolgung der geltenden Normen und Gesetze, zu überprüfen. Sämtliche der technischen Dokumentation zu entnehmenden Informationen werden ohne jegliche ausdrückliche, konkludente oder stillschweigende Garantie erteilt.

Im Übrigen gelten ausschließlich die Regelungen der jeweils aktuellen Allgemeinen Geschäftsbedingungen von Phoenix Contact, insbesondere für eine etwaige Gewährleistungshaftung.

Phoenix Contact behält sich das Recht vor, für die hier verwendeten Produktkennzeichnungen von Phoenix Contact-Produkten eigene Schutzrechte anzumelden. Die Anmeldung von Schutzrechten hierauf durch Dritte ist verboten.

Andere Produktkennzeichnungen können gesetzlich geschützt sein, auch wenn sie nicht als solche markiert sind.

So erreichen Sie uns

Internet

Aktuelle Informationen zu Produkten von Phoenix Contact und zu unseren Allgemeinen Geschäftsbedingungen finden Sie im Internet unter:
phoenixcontact.com.

Stellen Sie sicher, dass Sie immer mit der aktuellen Dokumentation arbeiten.
Diese steht unter der folgenden Adresse zum Download bereit:
phoenixcontact.net/products.

Ländervertretungen

Bei Problemen, die Sie mit Hilfe dieser Dokumentation nicht lösen können, wenden Sie sich bitte an Ihre jeweilige Ländervertretung.
Die Adresse erfahren Sie unter phoenixcontact.com.

Herausgeber

PHOENIX CONTACT GmbH & Co. KG
Flachsmarktstraße 8
32825 Blomberg
DEUTSCHLAND

Wenn Sie Anregungen und Verbesserungsvorschläge zu Inhalt und Gestaltung unseres Handbuchs haben, würden wir uns freuen, wenn Sie uns Ihre Vorschläge zusenden an:
tecdoc@phoenixcontact.com

PHOENIX CONTACT GmbH & Co. KG
Flachsmarktstraße 8
32825 Blomberg, Germany
Phone: +49 5235 3-00
Fax: +49 5235 3-41200
E-mail: info@phoenixcontact.com
phoenixcontact.com

108413_de_11
Order No. —11

INSPIRING INNOVATIONS