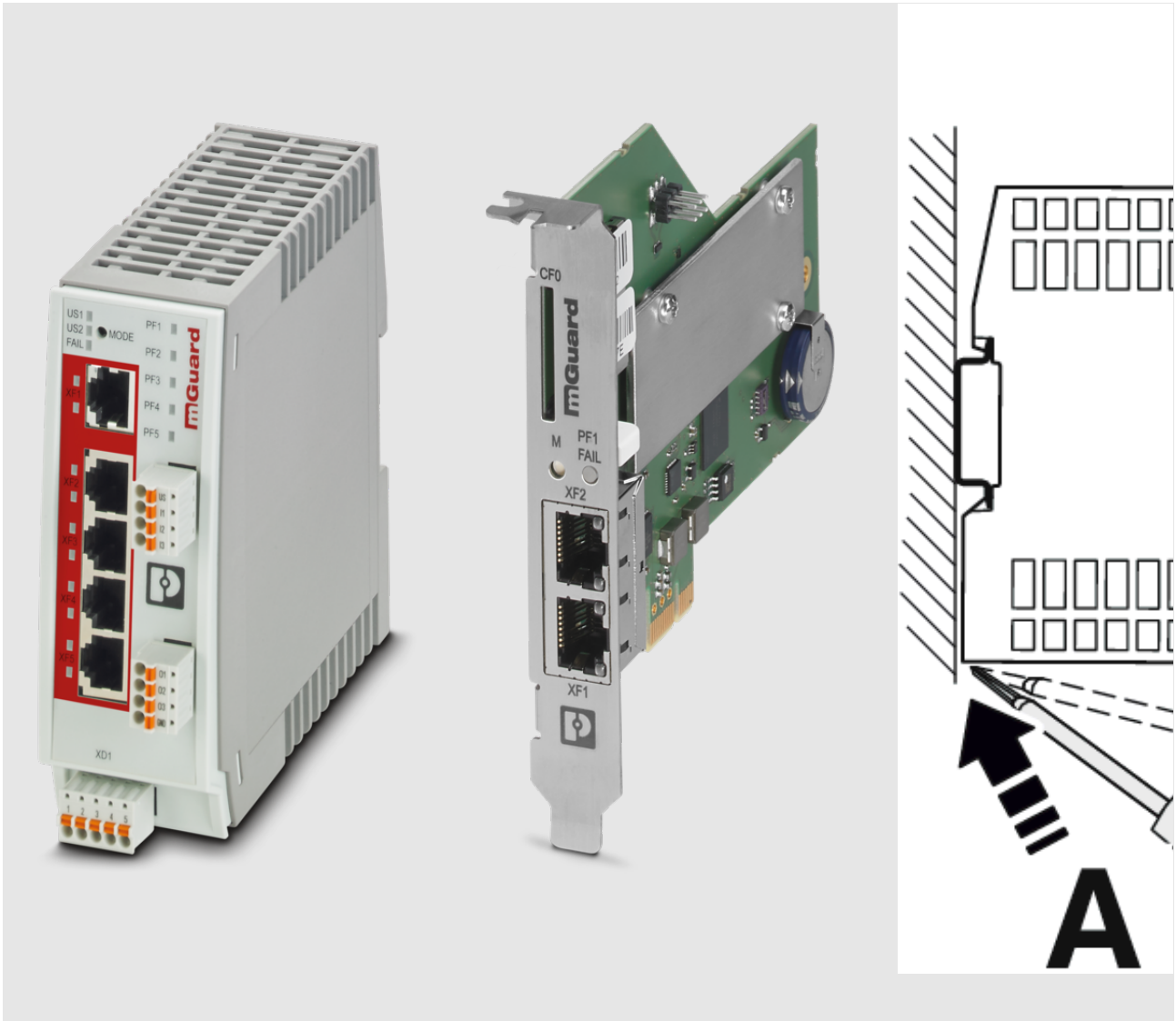


FL MGUARD 2000/4000
Installation und Inbetriebnahme

Anwenderhandbuch

Anwenderhandbuch
FL MGUARD 2000/4000 - Installation und Inbetriebnahme

UM DE HW FL MGUARD 2000/4000, Revision 08 2025-01-30

Dieses Handbuch ist gültig für:

Bezeichnung	Artikel-Nr.
FL MGUARD 2102	1357828
FL MGUARD 4302	1357840
FL MGUARD 4302/KX	1696708
FL MGUARD 2105	1357850
FL MGUARD 4305	1357875
FL MGUARD 4305/KX	1696779
FL MGUARD 4102 PCI	1441187
FL MGUARD 4102 PCIE	1357842

Firmware-Version: mGuard 10.5.x

Mitgeltende Dokumentation (verfügbar unter phoenixcontact.net/product/<artikel-nummer>):

Release Notes

mGuard 10.5.x Firmware – Release Notes

Benutzerhandbuch „Installation und Inbetriebnahme“

UM DE HW FL MGUARD 2000/4000 – 110192_de_xx

Benutzerhandbuch „Generic Administration Interface - gaiconfig User Guide“:

UM DE GAICONFIG MGUARD10 – 110193_de_xx

Benutzerhandbuch „Installation, Konfiguration und Benutzung des mGuard device manager (mdm)“:

UM DE MDM 1.17 – 111024_de_xx

Benutzerhandbuch „IEC 62443-4-2-konforme Konfiguration der FL MGUARD-Produktfamilie“:

UM DE MGUARD 62443-4-2 – 109049_de_xx

110192_de_08

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 sind industrietaugliche Security-Router mit integrierter Stateful-Packet-Inspection-Firewall und VPN. Sie eignen sich für die dezentrale Absicherung von Produktionszellen oder einzelner Maschinen gegen Manipulationen sowie für sichere Fernwartungsszenarien.
– Die Geräte sind nicht für den privaten Gebrauch bestimmt. Sie dürfen ausschließlich im gewerblichen bzw. industriellen Bereich eingesetzt und betrieben werden.

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

Um einen ordnungsgemäßen Betrieb und die Sicherheit der Umwelt und des Personals zu gewährleisten, muss das Gerät korrekt installiert, betrieben und gewartet werden.

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
Tragschienengeräte werden innerhalb eines Schaltschranks oder -kastens auf eine Norm-Tragschiene aufgerastet. Dieser Schaltschrank/-kasten muss den Anforderungen der IEC/EN 62368-1 bzgl. der Brandschutzumhüllung genügen.

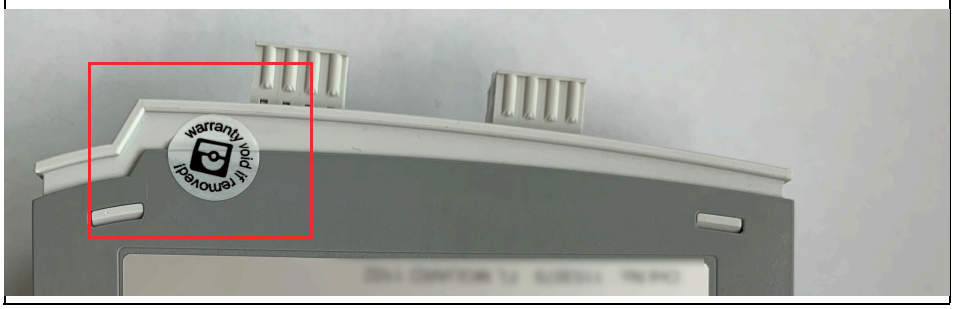
ACHTUNG: Anforderung an die Funktionserdung
Montieren Sie Tragschienengeräte auf einer geerdeten Tragschiene. Die Erdung des Moduls erfolgt mit dem Aufrasten auf die Tragschiene.

ACHTUNG: Anforderung an den Montageort
Die vorgeschriebene Einbaulage von Tragschienengeräten 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.

Um Manipulationen am gelieferten Gerät zu verhindern und ein unbefugtes Öffnen des Gerätes zu erkennen, wurde am Gehäuse von Hutschienengeräten und auf der Verpackung von PCI-Karten ein Sicherheitssiegel angebracht.

Prüfen Sie vor der Erstinbetriebnahme, ob das Siegel intakt ist. Im Falle einer Entfernung/Beschädigung des Siegels würden Teile des Siegels auf dem Gehäuse/der Verpackung verbleiben (siehe Kapitel 5).



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.

- Verdrahtung der Schnittstellen nur innerhalb von Gebäuden oder maximal 42,6 m außerhalb von Gebäuden.
- 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.

1.6.1 Sicherheitshinweise zur Installation in Zone 2 (nur Geräte mit Ex-Zulassung)

– Das Gerät der Kategorie 3 ist zur Installation im explosionsgefährdeten Bereich der Zone 2 geeignet. Es erfüllt die Anforderungen der EN 60079-0 und EN 60079-7.
– Das Gerät ist nicht für den Einsatz in staubexplosionsgefährdeten Atmosphären ausgelegt.
– Das Konfigurieren des Geräts mittels DIP-Schalter, Taster oder weiterer zugänglicher Schalter am Gerät ist nur außerhalb des explosionsgefährdeten Bereichs erlaubt.
– Halten Sie die festgelegten Bedingungen für den Einsatz in explosionsgefährdeten Bereichen ein. Setzen Sie bei der Installation ein geeignetes, zugelassenes Gehäuse der Mindestschutzart IP54 ein, das die Anforderungen der IEC/EN 60079-7 und GB/T 3836.1-2010 erfüllt. Beachten Sie auch die Anforderungen der IEC/EN 60079-14.
– An Stromkreise der Zone 2 dürfen nur Geräte angeschlossen werden, die für den Betrieb in der Ex-Zone 2 und die am Einsatzort vorliegenden Bedingungen geeignet sind.
– Das Trennen und Verbindungen von Leitungen, SFP-Modulen und SD-Karten im explosionsgefährdeten Bereich ist nur im spannungslosen Zustand zulässig.
– Verwenden Sie nur einwandfreie Ethernet-Leitungen mit funktionierender Verrastung.
– Steckbare Verbindungen (z. B. Stecker, SD-Karte) müssen eine funktionsfähige Verriegelung aufweisen (z. B. Rasthaken, Verschraubung). Setzen Sie die Verriegelung ein und setzen Sie beschädigte Verriegelungen unverzüglich instand. Stellen Sie sicher, dass alle steckbaren Verbindungen vollständig eingesteckt sind.
– Das Gerät ist außer Betrieb zu nehmen und unverzüglich aus dem Ex-Bereich zu entfernen, wenn es beschädigt ist, unsachgemäß belastet oder gelagert wurde bzw. Fehlfunktionen aufweist.
– Die Umgebungstemperatur innerhalb des Endverbrauchergehäuses muss innerhalb von 25 mm zum Gerät gemessen und eingehalten werden.
– Schließen Sie nur eine Leitung pro Klemmpunkt an.
– Der Luftdruck im Betrieb ist begrenzt auf 108 kPa.
– Galvanische Isolierung, 500 V AC nach EN/IEC 60079-7. Beachten Sie die Einschränkungen in den besonderen Verwendungsbedingungen.
– Zwischen den Spannungsversorgungsanschlüssen und FE leiten Überspannungsableiter Störungen <500 V_{eff} ab. Ziehen Sie deshalb vor der Isolationsmessung den Spannungsversorgungsstecker ab. Andernfalls sind Isolationsfehlmessungen möglich. Setzen Sie den Stecker nach der Isolationsmessung wieder in die vorgesehene Buchse ein.

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 15.12.2024):

– 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.

Stellen Sie die Integrität von heruntergeladenen Dateien sicher

Phoenix Contact stellt Prüfsummen der Dateien bereit, die über die Produktseite des jeweiligen Geräts heruntergeladen werden können.

- Um sicherzugehen, dass die heruntergeladenen Firmware- oder Update-Dateien als auch heruntergeladene Dokumentation während des Downloads nicht von Dritten verändert wurden, vergleichen Sie die SHA256-Prüfsummen der Dateien mit den auf der entsprechenden Produktseite (phoenixcontact.com/product/<Bestellnummer>) angegebenen Prüfsummen.

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, 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 „*Web-based Management*“ (UM DE FW MGUARD10) beschrieben. Erhältlich im Download-Bereich der entsprechenden Produktseite im Phoenix Contact Web-Shop, z. B. unter phoenixcontact.net/product/1357828.

2 Übersicht FL MGUARD 2000/4000-Serie

2.1 Produktübersicht

Mit den Geräten der FL MGUARD 2000/4000-Serie wird die etablierte FL MGUARD RS2000/4000-Serie um neue Modelle erweitert. Die neuen Modelle (Geräteplattform MGUARD3) verfügen über schnelles Gigabit-Ethernet.

Die Unterschiede zwischen den Geräte-Serien sowie die Möglichkeit der Übertragung von Konfigurationen auf Geräte der neue FL MGUARD 2000/4000-Serie werden in Kapitel 2.2 beschrieben.

Produktübersicht und Varianten

Wenn nicht anders angegeben, sind in diesem Dokument bei der Nennung der Geräte FL MGUARD 4302 und FL MGUARD 4305 die Varianten 4302/KX und 4305/KX ebenfalls mitgemeint.

Tabelle 2-1 Produktübersicht und Artikelnummern

Gerät	Kurzbeschreibung	Artikel-nummer
FL MGUARD 2102	Tragschienengerät, 2 x RJ45-Ports, SD-Kartenhalter, digitale Service I/Os, Gigabit-Ethernet	1357828
FL MGUARD 4302	Tragschienengerät, 2 x RJ45-Ports, SD-Kartenhalter, digitale Service I/Os, Gigabit-Ethernet, redundante Stromversorgung	1357840
FL MGUARD 4302/KX	Tragschienengerät, 2 x RJ45-Ports, SD-Kartenhalter, digitale Service I/Os, Gigabit-Ethernet, redundante Stromversorgung, Ex-Zulassung	1696708
FL MGUARD 2105	Tragschienengerät, 5 x RJ45-Ports, Ethernet-Switch (unmanaged), SD-Kartenhalter, digitale Service I/Os, Gigabit-Ethernet	1357850
FL MGUARD 4305	Tragschienengerät, 5 x RJ45-Ports, Ethernet-Switch (managed), SD-Kartenhalter, digitale Service I/Os, Gigabit-Ethernet, redundante Stromversorgung	1357875
FL MGUARD 4305/KX	Tragschienengerät, 5 x RJ45-Ports, Ethernet-Switch (managed), SD-Kartenhalter, digitale Service I/Os, Gigabit-Ethernet, redundante Stromversorgung, Ex-Zulassung	1696779
FL MGUARD 4102 PCI	PCI-Karte, 2 x RJ45-Ports, SD-Kartenhalter, Gigabit-Ethernet	1441187
FL MGUARD 4102 PCIE	PCI-Express-Karte,2 x RJ45-Ports, SD-Kartenhalter, Gigabit-Ethernet	1357842

Einsatzbereich

Die Geräte der FL MGUARD 4000-Serie sind Security-Router mit intelligenter Stateful-Packet-Inspection-Firewall und integriertem IPsec-VPN und OpenVPN mit bis zu 250 VPN-Tunneln. Sie sind für den Einsatz in der Industrie mit hohen Ansprüchen an dezentrale Sicherheit und Hochverfügbarkeit konzipiert.

Die Geräte der FL MGUARD 2000-Serie sind eine Variante mit einfacher Firewall und integriertem IPsec-VPN und OpenVPN mit maximal 2 VPN-Tunneln. Der Funktionsumfang ist auf das Wesentliche reduziert. Die Geräte eignen sich für sichere Fernwartungsszenarien in der Industrie und ermöglichen eine schnelle Inbetriebnahme von robusten, industrietauglichen Feldgeräten für einen störungsfreien, autarken Betrieb.

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.

PROFINET RT

Die Geräte FL MGUARD 210X/410X/430X sind hardwaretechnisch so gestaltet, dass die WAN-Seite (Interface XF1) und die LAN-Seite (Interface XF2 bzw. XF2-XF5) über den Applikationsprozessor sicher voneinander getrennt sind.

Zudem ist die mGuard-Firmware 10.x so implementiert, dass eine Übertragung von Layer 2-Datagrammen wie z. B. PROFINET RT bei Nutzung des Netzwerk-Modus „Router“ (Werkseinstellung) ausgeschlossen ist.

mGuard-Geräte können somit als sichere Netzwerkgrenze für PROFINET verwendet werden. Sie können als Schutzgeräte für PROFIsafe-Netzwerkzellen, in Umgebungen, in denen eine Eindeutigkeit der PROFIsafe-Adressen nicht sichergestellt werden kann, verwendet werden.

Der Einsatz der Geräte erfolgt hierbei konform zur Norm IEC 61784-3-3 (5.4.2 und 8.1.2).

2.2 Neue Geräteplattform FL MGUARD 2000/4000

Mit den Geräten der FL MGUARD 2000/4000-Serie werden die etablierten mGuard-Geräte der RS2000/RS4000- und PCI(E)4000-Serie nach und nach ersetzt.

Die neuen Geräte mit bewährter *mGuard Security Technology* sind mit schnellem Gigabit-Ethernet ausgestattet und werden mit der Firmwareversion mGuard 10.x betrieben.

Die Geräte sind kompatibel zu ihren Vorgängermodellen, können bestehende Konfigurationsprofile (atv-Dateien) importieren und über CGI- und GAI-Schnittstellen konfiguriert werden.

Der mGuard device manager kann zur **Verwaltung** von mGuard-Geräten mit installierter Firmware-Version bis mGuard 10.5.x verwendet werden (siehe Benutzerhandbuch „FL MGUARD DM UNLIMITED“ – 111024_de_xx).

Aktuell können einige Gerätefunktionen der Vorgängermodelle auf den neuen Modellen noch nicht unterstützt werden (siehe Kapitel 2.2.1).

2.2.1 Nicht mehr unterstützte Funktionen

Auf der neuen Geräteplattform werden bestimmte Funktionen der alten Geräteplattform nicht mehr unterstützt.

Hardware

Die neuen mGuard-Modelle der FL MGUARD 2000/4000-Serie werden ohne serielle Schnittstelle und ohne internes Modem angeboten.

Die Anschlüsse für die Spannungsversorgung sowie digitale Ein- und Ausgänge werden bei Tragschienegeräten in Form von COMBICON-Steckverbindern bereitgestellt (siehe Kapitel 3.3).

Firmware (Funktionen)

Einige bisher verfügbare Gerätefunktionen werden auf den Geräten der FL MGUARD 2000/4000-Serie derzeit nicht unterstützt (siehe Tabelle 2-2).

Tabelle 2-2 Aktuelle Funktionsunterschiede

Funktionen, die in der Firmware mGuard 10.5.x aktuell nicht unterstützt werden
Netzwerk: Interfaces – PPPoE – PPTP – Sekundäres externes Interface
Netzwerk: Serielle Schnittstelle
Generic Routing Encapsulation (Netzwerk >> GRE-Tunnel)
VPN-Redundanz
Quality of Services (QoS)
CIFS-Integrity-Monitoring
SEC-Stick

Bei der Übertragung von älteren Gerätekonfigurationen auf die neuen Geräte muss deshalb darauf geachtet werden, dass die in Tabelle 2-2 beschriebenen Funktionen vor dem Export in der Gerätekonfiguration deaktiviert bzw. auf Werkseinstellungen zurückgesetzt wurden (siehe auch Kapitel 2.2.2).

2.2.2 Migration der Gerätekonfiguration

Die Migration der Konfiguration älterer mGuard-Geräte kann über das Web-based Management (WBM) oder via SD-Karte (ECS) vorgenommen werden.

Voraussetzungen

Sind Gerätefunktionen des Geräts, dessen Konfiguration migriert werden soll, auf dem neuen Gerät nicht verfügbar, müssen die Variablen vor dem Export der Konfiguration auf dem alten Gerät auf Werkseinstellungen zurückgesetzt werden (siehe Tabelle 2-2).

Das genaue Vorgehen bei der Gerätemigration wird im Dokument 111259_de_xx (AH DE MGUARD MIGRATE 10) beschrieben, erhältlich unter phoenixcontact.com/product/1357875.

Weitere Informationen finden Sie im aktuellen Anwenderhandbuch „Web-based Management“ UM DE FW MGUARD10 – 110191_de_xx.

2.3 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.

2.3.1 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.
- Prüfen Sie, ob das Sicherheitssiegel intakt ist. Im Falle einer Entfernung/Beschädigung des Siegels würden Teile des Siegels auf dem Gehäuse/der Verpackung verbleiben (siehe Kapitel 5).
- 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 7, falls die Originalverpackung nicht mehr vorliegt.

2.4 Werkseinstellungen

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

2.4.1 Netzwerkinterfaces

Die grundlegenden Netzwerkfunktionen (Ethernet) des Geräts sind nach dem Start des Geräts verfügbar (siehe Tabelle 2-3).

Eine Konfiguration des Geräts über das WAN-Interface ist nicht möglich, da der externe Zugriff auf das Gerät durch die Firewall blockiert wird (siehe Kapitel 2.4.5).

Tabelle 2-3 **Werkseinstellungen**: Konfiguration der Netzwerkinterfaces

Funktion	WAN (XF1)	LAN (XF2-4 bzw. XF2-5) (je nach Gerätetyp)	DMZ (XF5) (nur FL MGUARD 4305)
IP-Adresse (IPv4)	Wird automatisch zugewiesen, wenn ein DHCP-Server im externen Netzwerk vorhanden ist.	192.168.1.1	-
Netzmaske		24	-
Standard-Gateway	Kann optional vom DHCP-Server zugewiesen werden.	–	-
IP-Masquerading (NAT)	Wird auf alle gerouteten Datenpakete angewendet, die das Gerät über das Netzwerkinterface XF1 (in das externe WAN-Netzwerk) verlassen.	–	-

2.4.2 Benutzerzugriff

Der Zugriff auf die Benutzerinterfaces WBM und Shell-Zugang (SSH) erfolgt unter der Angabe von Benutzername und Passwort.

Benutzername	Passwort
root	*root*
admin	*mGuard*

Ändern Sie bei der Erstinbetriebnahme des Geräts umgehend die voreingestellten Administrator-Passwörter.

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

2.4.3 Aktive Netzwerkdienste (Gerät als Client)

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

Tabelle 2-4 **Werkseinstellungen**: Aktive Dienste (als Client)

Dienst/Service	Aktiv über	Konfiguration (Werkseinstellungen)
DHCP-Client	WAN-Interface (XF1)	Sendet DHCP-Anfragen über UDP-Port 67.
DNS-Client	WAN-Interface (XF1)	Sendet DNS-Anfragen an DNS-Root-Nameserver über UDP-Port 53.
NTP-Client	deaktiviert	

2.4.4 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 2-5 **Werkseinstellungen**: Aktive Dienste (als Server)

Dienst/Service	Erreichbar über	Konfiguration (Werkseinstellungen)
Webserver (HTTPS)	LAN (XF2-5) (nicht FL MGUARD 4305) LAN (XF2-4) (FL MGUARD 4305)	Anfrage über TCP-Port 443 (HTTPS) Clients, die über das LAN-Interface mit dem Gerät verbunden sind, können auf das Web-based Management zugreifen.
Kommandozeile / GAI (SSH)	LAN (XF2-5) (nicht FL MGUARD 4305) LAN (XF2-4) (FL MGUARD 4305)	Anfrage über SSH-Port 22 (SSH) Clients, die über das LAN-Interface mit dem Gerät verbunden sind, können über die Kommandozeile auf das *Generic Administration Interface* (GAI) zugreifen.
DHCP-Server	LAN (XF2-5) (nicht FL MGUARD 4305) LAN (XF2-4) (FL MGUARD 4305)	Anfrage über UDP-Port 67 Clients, die über das LAN-Interface mit dem Gerät verbunden sind, können eine Netzwerkkonfiguration von dessen DHCP-Server anfordern (Internes DHCP). 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/WINS-Server: 192.168.1.1

Tabelle 2-5 **Werkseinstellungen**: Aktive Dienste (als Server)

Dienst/Service	Erreichbar über	Konfiguration (Werkseinstellungen)
DNS-Server	LAN (XF2-5) (nicht FL MGUARD 4305) LAN (XF2-4) (FL MGUARD 4305)	Anfrage über TCP/UDP-Port 53 Clients, die über das LAN-Interface mit dem Gerät verbunden sind, können Anfragen zur Namensauflösung an dessen DNS-Server senden.
SNMP-Server	deaktiviert	
NTP-Server	deaktiviert	

2.4.5 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 (z. B. Gerätezugriff).
- **Durchgehender Datenverkehr** bezieht sich auf die Pakete, die durch das Gerät durchgeleitet (*geroutet*) werden, z. B. eingehend über LAN (XF2) und ausgehend über WAN (XF1).

Firewall (für eingehenden Datenverkehr) = Gerätezugriff

Tabelle 2-6 **Werkseinstellungen**: Firewall für eingehenden Datenverkehr

Dienst/ Service, Protokoll	Eingehend über	Status	Port	Beschreibung
HTTPS	LAN (XF2-5) (nicht FL MGUARD 4305) LAN (XF2-4) (FL MGUARD 4305)	✓	TCP 443	Entsprechende Anfragen an den Webserver des Geräts sind **erlaubt**: – Anmeldung und Konfiguration via Web-based Management
	WAN (XF1)	⊘		Anfragen über das WAN-Interface werden verworfen.
SSH	LAN (XF2-5) (nicht FL MGUARD 4305) LAN (XF2-4) (FL MGUARD 4305)	✓	SSH 22	Entsprechende Anfragen an den SSH-Server des Geräts sind **erlaubt**: – Shell-Zugang – Konfiguration via GAI-Config
	WAN (XF1)	⊘		Anfragen über das WAN-Interface werden verworfen.
DHCP	LAN (XF2-5) (nicht FL MGUARD 4305) LAN (XF2-4) (FL MGUARD 4305)	✓	UDP 67	Entsprechende Anfragen an den DHCP-Server des Geräts sind **erlaubt**.
	WAN (XF1)	⊘		Anfragen über das WAN-Interface werden verworfen.
DNS	LAN (XF2-5) (nicht FL MGUARD 4305) LAN (XF2-4) (FL MGUARD 4305)	✓	TCP 53 UDP 53	Entsprechende Anfragen an den DNS-Server des Geräts sind **erlaubt**.
	WAN (XF1)	⊘		Anfragen über das WAN-Interface werden verworfen.
ICMP **(IPv4)**	LAN (XF2-5) (nicht FL MGUARD 4305) LAN (XF2-4) (FL MGUARD 4305)	✓		Ping-Anfragen an die konfigurierte IPv4-Adresse der Netzwerk-Interfaces sind erlaubt.
	WAN (XF1)	⊘		Anfragen über das WAN-Interface werden verworfen.

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

Werkseinstellungen: Firewall (durchgeleiteter Datenverkehr: Paketfilter >> Ausgangsregeln)

Alle Pakete, die aus dem LAN-Netzwerk (XF2-5 bzw. XF2-4) an beliebige Zieladressen gesendet werden, werden vom Gerät weitergeleitet.

Werkseinstellungen: Firewall (durchgeleiteter Datenverkehr: Paketfilter >> Eingangsregeln)

Alle Pakete, die aus dem WAN-Netzwerk (XF1) an beliebige Zieladressen gesendet werden, werden vom Gerät verworfen.

3 FL MGUARD 2102/2105 und 4302/4305

Tabelle 3-1 Aktuell verfügbare Produkte

Produktbezeichnung	Artikelnummer
FL MGUARD 2102	1357828
FL MGUARD 4302	1357840
FL MGUARD 4302/KX	1696708
FL MGUARD 2105	1357850
FL MGUARD 4305	1357875
FL MGUARD 4305/KX	1696779

Produktbeschreibung

FL MGUARD 4000: Die Geräte der FL MGUARD 4000-Serie sind Security-Router mit intelligenter Stateful-Packet-Inspection-Firewall und integriertem IPsec-VPN und OpenVPN mit bis zu 250 VPN-Tunneln. Sie sind für den Einsatz in der Industrie mit hohen Ansprüchen an dezentrale Sicherheit und Hochverfügbarkeit konzipiert.

Beim **FL MGUARD 4305** ermöglicht ein dedizierter DMZ-Port mit eigenen Firewall-Regeln eine Segmentierung und differenziertere Sicherheitskonzepte.

Die Varianten **FL MGUARD 4302/KX** und **FL MGUARD 4305/KX** sind für explosionsgefährdete Bereiche der Zone 2 zugelassen (Ex-Zulassung). Sie sind bei der Nennung der Geräte FL MGUARD 4302 und FL MGUARD 4305 grundsätzlich mitgemeint.

FL MGUARD 2000: Die Geräte der FL MGUARD 2000-Serie sind eine Variante mit einfacher Firewall und integriertem IPsec-VPN und OpenVPN mit maximal 2 VPN-Tunneln. Der Funktionsumfang ist auf das Wesentliche reduziert. Die Geräte eignen sich für sichere Fernwartungsszenarien in der Industrie und ermöglichen eine schnelle Inbetriebnahme von robusten, industrietauglichen Feldgeräten für einen störungsfreien, autarken Betrieb.

Bild 3-1 FL MGUARD 2102/4302 (links) und FL MGUARD 2105/4305 (rechts)

3.1 Gerätebeschreibung

3.1.1 FL MGUARD 2102 / FL MGUARD 4302 (/KX)

Das Gerät verfügt über folgende Netzwerkanschlüsse:

– **Netzwerkinterface XF1 / WAN**: Ethernet 10/100/1000 Mbit/s (RJ45-Port)
– **Netzwerkinterface XF2 / LAN**: Ethernet 10/100/1000 Mbit/s (RJ45-Port)

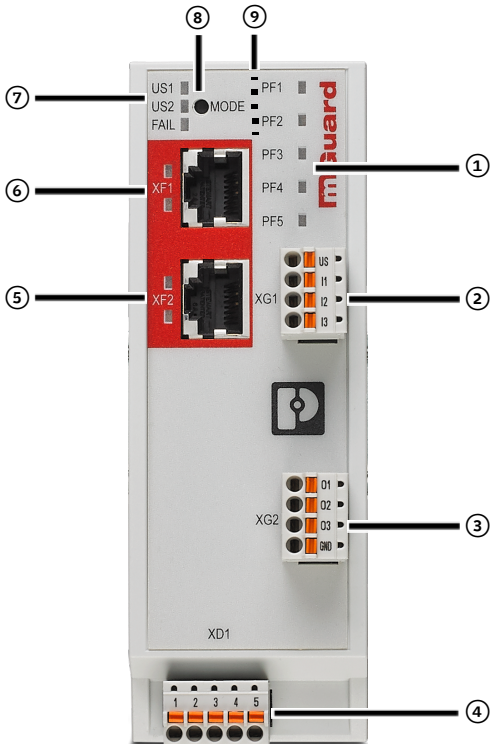


Bild 3-2 FL MGUARD 2102 / FL MGUARD 4302: Bedienelemente und Anzeigen

① Status- und Diagnose-LEDs
(siehe Kapitel 3.2.1)

② Anschluss digitaler **Eingänge** über COMBICON-Steckverbindung (Push-in-Kontakt)
(siehe Kapitel 3.6)

③ Anschluss digitaler **Ausgänge** über COMBICON-Steckverbindung (Push-in-Kontakt)
(siehe Kapitel 3.6)

④ Anschluss der Versorgungsspannung über COMBICON-Steckverbindung (Push-in-Kontakt)
(siehe Kapitel 3.4)

⑤ Netzwerkinterface XF2/**LAN** (RJ45-Ethernet-Port) (siehe Kapitel 3.5)
LED LNK/ACT (oben) | LED SPD (unten)
(siehe Kapitel 3.2.2)

⑥ Netzwerkinterface XF1/**WAN** (RJ45-Ethernet-Port) (siehe Kapitel 3.5)
LED LNK/ACT (oben) | LED SPD (unten)
(siehe Kapitel 3.2.2)

⑦ Status- und Diagnose-LEDs
(siehe Kapitel 3.2.3, 3.2.4)

⑧ Mode-Taste
(siehe Kapitel 6)

⑨ SD-Kartenhalter (auf der Rückseite des Geräts) (siehe Kapitel 3.7)

3.1.2 FL MGUARD 2105

Das Gerät verfügt über folgende Netzwerkanschlüsse:

– **Netzwerkinterface XF1 / WAN**: Ethernet 10/100/1000 Mbit/s (RJ45-Port)
– **Netzwerkinterface XF2-5 / LAN**: 4-Port-Ethernet-Switch 10/100/1000 Mbit/s (RJ45-Port)

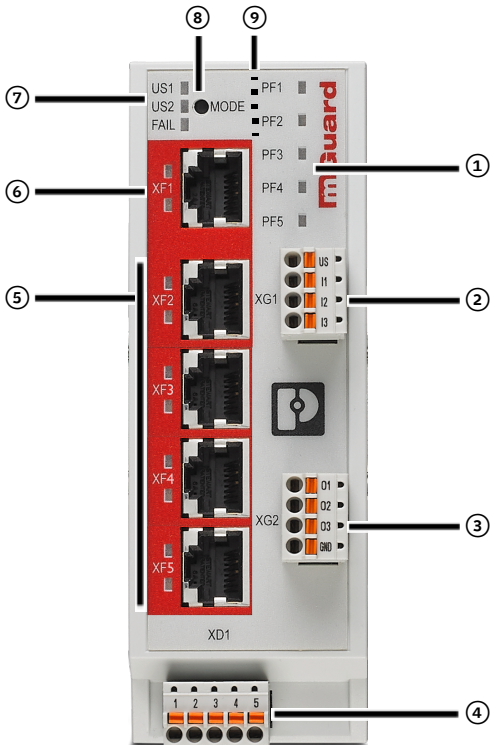


Bild 3-3 FL MGUARD 2105: Bedienelemente und Anzeigen

① Status- und Diagnose-LEDs
(siehe Kapitel 3.2.1)

② Anschluss digitaler **Eingänge** über COMBICON-Steckverbindung (Push-in-Kontakt)
(siehe Kapitel 3.6)

③ Anschluss digitaler **Ausgänge** über COMBICON-Steckverbindung (Push-in-Kontakt)
(siehe Kapitel 3.6)

④ Anschluss der Versorgungsspannung über COMBICON-Steckverbindung (Push-in-Kontakt)
(siehe Kapitel 3.4)

⑤ Netzwerkinterface XF2-5/**LAN** (4x RJ45-Ethernet-Port / Netzwerk-Switch) (siehe Kapitel 3.5)
LED LNK/ACT (oben) | LED SPD (unten)
(siehe Kapitel 3.2.2)

⑥ Netzwerkinterface XF1/**WAN** (RJ45-Ethernet-Port) (siehe Kapitel 3.5)
LED LNK/ACT (oben) | LED SPD (unten)
(siehe Kapitel 3.2.2)

⑦ Status- und Diagnose-LEDs
(siehe Kapitel 3.2.3, 3.2.4)

⑧ Mode-Taste
(siehe Kapitel 6)

⑨ SD-Kartenhalter (auf der Rückseite des Geräts)
(siehe Kapitel 3.7)

3.1.3 FL MGUARD 4305

Das Gerät verfügt über folgende Netzwerkanschlüsse:

– **Netzwerkinterface XF1 / WAN**: Ethernet 10/100/1000 Mbit/s (RJ45-Port)
– **Netzwerkinterface XF2-4 / LAN**: 3-Port-Ethernet-Switch 10/100/1000 Mbit/s (RJ45-Port)
– **Netzwerkinterface XF5 / DMZ**: Ethernet 10/100/1000 Mbit/s (RJ45-Port)

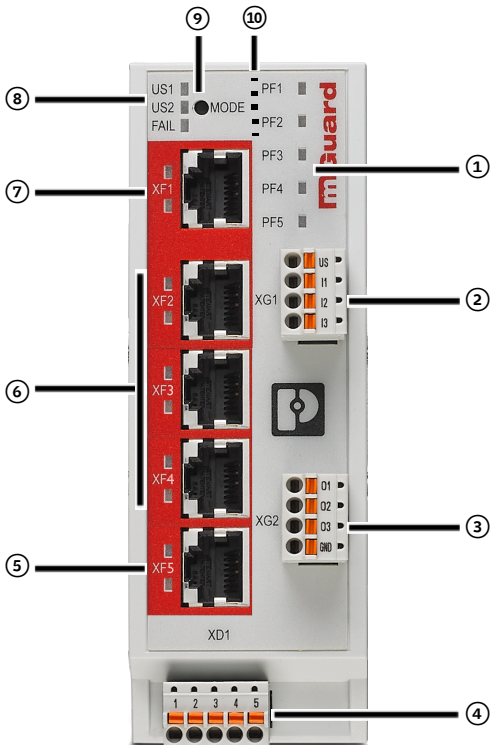


Bild 3-4 FL MGUARD 2105: Bedienelemente und Anzeigen

① Status- und Diagnose-LEDs
(siehe Kapitel 3.2.1)

② Anschluss digitaler **Eingänge** über COMBICON-Steckverbindung (Push-in-Kontakt)
(siehe Kapitel 3.6)

③ Anschluss digitaler **Ausgänge** über COMBICON-Steckverbindung (Push-in-Kontakt)
(siehe Kapitel 3.6)

④ Anschluss der Versorgungsspannung über COMBICON-Steckverbindung (Push-in-Kontakt)(siehe Kapitel 3.4)

⑤ Netzwerkinterface XF5/**DMZ** (RJ45-Ethernet-Port) (siehe Kapitel 3.5)
LED LNK/ACT (oben) | LED SPD (unten)
(siehe Kapitel 3.2.2)

⑥ Netzwerkinterface/Switch XF2-4/**LAN** (3x RJ45-Ethernet-Port) (siehe Kapitel 3.5)
LED LNK/ACT (oben) | LED SPD (unten)
(siehe Kapitel 3.2.2)

⑦ Netzwerkinterface XF1/**WAN** (RJ45-Ethernet-Port) (siehe Kapitel 3.5)
LED LNK/ACT (oben) | LED SPD (unten)
(siehe Kapitel 3.2.2)

⑧ Status- und Diagnose-LEDs
(siehe Kapitel 3.2.3, 3.2.4)

⑨ Mode-Taste
(siehe Kapitel 6)

⑩ SD-Kartenhalter (auf der Rückseite des Geräts)
(siehe Kapitel 3.7)

3.2 LED – Status- und Diagnoseanzeige

Mithilfe der Status- und Diagnose-LEDs werden unterschiedliche System- und Fehlerzustände des Geräts angezeigt (siehe Kapitel 3.2.5).

3.2.1 PF1 – PF5

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

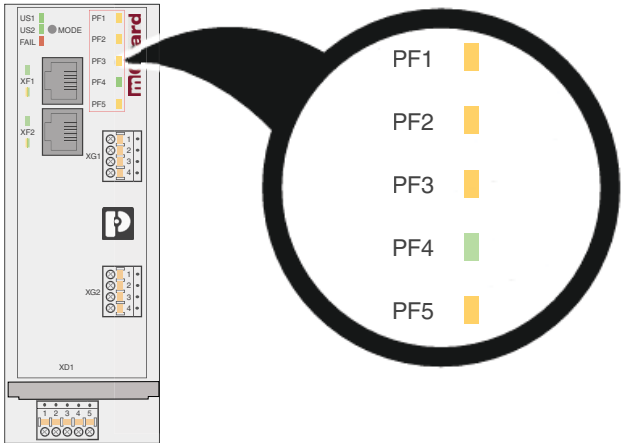


Bild 3-5 LED: PF1 – PF5

Tabelle 3-2 LED: PF1 – PF5: Geräte-Status (Beispiele)

Geräte-Status			
Wird gestartet	**Betriebsbereit**	**VPN-Verbindung / Firewall-Regelsatz** Überwacht über die Servicekontakte O1 und O2	**VPN-Verbindung / Firewall-Regelsatz** Überwacht über die Servicekontakte O1 und O2
PF1 PF2 PF3 PF4 **PF5**	PF1 PF2 PF3 PF4 PF5	PF1 PF1 PF2 PF2 PF3 PF3 **PF4** **PF4** PF5 PF5	PF1 PF1 PF2 PF2 **PF3** PF3 PF4 **PF4** PF5 PF5
Das Gerät wird gestartet. Bei Gerätestart leuchten alle PF-LEDs kurz auf (orange).	Das Gerät wurde vollständig gestartet. Die LED PF1 blinkt im Rhythmus eines Herzschlags.	Die VPN-Verbindung/der Firewall-Regelsatz wird aufgebaut/aktiviert. O1: Die LED PF3 blinkt O2: Die LED PF4 blinkt	Die VPN-Verbindung/der Firewall-Regelsatz wurde aufgebaut/aktiviert. O1: Die LED PF3 leuchtet O2: Die LED PF4 leuchtet

3.2.2 LNK/ACT und SPD

Die LEDs LNK/ACT (*Link/Activity)* und SPD (*Speed*) zeigen den Status der Netzwerkverbindung des zugehörigen Netzwerkports an (siehe Tabelle 3-3).

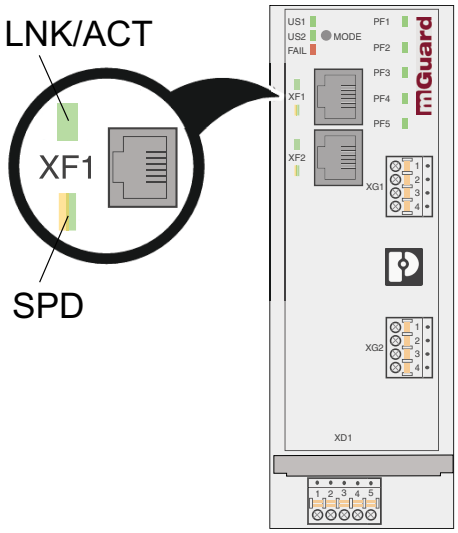


Bild 3-6 LED: LNK/ACT und SPD

Tabelle 3-3 LED: LNK/ACT und SPD (FL MGUARD 2102/4302)

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) **oder** Inaktiv - keine Datenübertragung (wenn LED LNK/ACT nicht aktiv)

3.2.3 US1 und US2

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

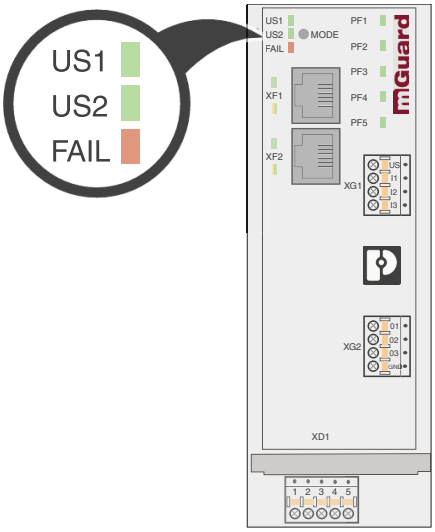


Bild 3-7 LED: US1 and US2

Tabelle 3-4 LED: US1 and US2

Bezeichnung	Farbe	Status	Bedeutung
US1	Grün	An	Versorgungsspannung liegt im Toleranzbereich (siehe Kapitel 8)
		Aus	Versorgungsspannung nicht vorhanden oder zu niedrig (siehe Kapitel 8)
US2 (nur FL MGUARD 4300-Serie)	Grün	An	Versorgungsspannung liegt im Toleranzbereich (siehe Kapitel 8)
		Aus	Versorgungsspannung nicht vorhanden oder zu niedrig (siehe Kapitel 8)
Nur Geräte der FL MGUARD 4000-Serie verfügen über eine redundante Spannungsversorgung.			

3.2.4 FAIL

Die LED FAIL zeigt verschiedene Status und Fehlerzustände des Geräts an (siehe Kapitel 3.2.5).

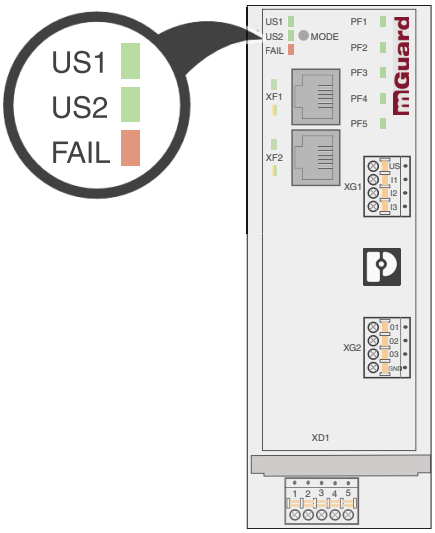


Bild 3-8 LED: FAIL

3.2.5 Darstellung der Systemzustände

Die Systemzustände (Status-, Alarm- oder Fehlermeldungen), die über das Leucht- bzw. Blinkverhalten der LED-Dioden angezeigt werden, entnehmen Sie bitte Tabelle 3-5.

Weitere Informationen zu Fehler- und Systemzuständen entnehmen Sie bitte auch den entsprechenden Log-Dateien.

Tabelle 3-5 Durch das Leucht- und Blinkverhalten der LEDs dargestellte Systemzustände

PF1 (grün)	PF2 (grün)	PF3 (grün)	PF4 (grün)	PF5 (ERR) (rot)	FAIL (FAULT) (rot)	Beschreibung des Systemzustands
Betriebsbereitschaft						
Herz-schlag						Der Systemstatus ist OK. Die LED PF1 blinkt im Rhythmus „Herzschlag“.
Systemstart						
Herz-schlag				ON (ca. 20 sec)	**ON** (ca. 20 sec)	Das System bootet. Alle LEDs der Ethernet-Ports (LNK/ACT und SPD) leuchten kurz rot/grün. Alle PF-LEDs (PF1–5) leuchten kurz orange. Die LED PF1 blinkt im Rhythmus „Herzschlag“.
Herz-schlag				Blink 500/500	ON	Das Starten des Gerätes ist nach einer Integritäts-prüfung des Dateisystems fehlgeschlagen. Das Dateisystem ist beschädigt oder wurde manipu-liert. Das Gerät kann nur durch einen Rescue Flash wieder in Betrieb genommen werden.
Herz-schlag	ON (orange) (3 sec)					ECS: Die Konfiguration wurde erfolgreich vom ECS geladen und angewendet.
Update						
				Blink 500/500		Der Austausch des Bootloaders ist aufgrund eines Hardwaredefekts fehlgeschlagen.
				Blink 500/500		Ein anderer schwerer Fehler ist aufgetreten.
Funktions-Überwachung / Alarmausgang						
Herz-schlag					ON	Keine Konnektivität auf der WAN-Schnittstelle (Linküberwachung am Gerät konfigurierbar)
Herz-schlag					ON	Keine Konnektivität auf der LAN-Schnittstelle (Lin-küberwachung am Gerät konfigurierbar)
Herz-schlag					ON	Spannungsversorgung 1 oder 2 ausgefallen (Alarm am Gerät konfigurierbar)
Herz-schlag					ON	Temperatur zu hoch / zu niedrig (Alarm am Gerät konfigurierbar)
Herz-schlag					ON	(Redundanz) Verbindungsprüfung fehlgeschlagen (Alarm am Gerät konfigurierbar)

Tabelle 3-5 Durch das Leucht- und Blinkverhalten der LEDs dargestellte Systemzustände

PF1 (grün)	PF2 (grün)	PF3 (grün)	PF4 (grün)	PF5 (ERR) (rot)	FAIL (FAULT) (rot)	Beschreibung des Systemzustands
Herz-schlag					ON	Administrator-Passwörter nicht konfiguriert (Alarm am Gerät konfigurierbar)
Schaltbare VPN-Verbindungen/Firewall-Regelsätze (über Servicekontakte)						
Herz-schlag		Blink				**Servicekontakt O1:** Die über den Servicekontakt O1 geschaltete VPN-Verbindung wird aufgebaut.
Herz-schlag		ON				**Servicekontakt O1:** Die über den Servicekontakt O1 geschaltete VPN-Verbindung wurde erfolgreich aufgebaut. ODER **Servicekontakt O1:** Der über den Servicekontakt O1 geschaltete Firewall-Regelsatz wurde erfolgreich aktiviert .
Herz-schlag			Blink			**Servicekontakt O2:** Die über den Servicekontakt O2 geschaltete VPN-Verbindung wird aufgebaut.
Herz-schlag			ON			**Servicekontakt O2:** Die über den Servicekontakt O2 geschaltete VPN-Verbindung wurde erfolgreich aufgebaut. ODER **Servicekontakt O2:** Der über den Servicekontakt O2 geschaltete Firewall-Regelsatz wurde erfolgreich aktiviert.
Externer Konfigurationsspeicher (ECS)						
Herz-schlag	ON (orange) (3 sec)					ECS: Die Konfiguration wurde erfolgreich vom ECS geladen und angewendet.
Herz-schlag				ON (3 sec)		ECS: Das ECS ist inkompatibel.
Herz-schlag				ON (3 sec)		ECS: Die Kapazität des ECS ist erschöpft.
Herz-schlag				ON (3 sec)		ECS: Das Root-Passwort aus dem ECS stimmt nicht überein.
Herz-schlag				ON (3 sec)		ECS: Die Konfiguration konnte nicht aus dem ECS geladen werden.
Herz-schlag				ON (3 sec)		ECS: Die Konfiguration konnte nicht im ECS gespeichert werden.
Recovery-Prozedur						
Herz-schlag				ON (2 sec)		RECOVERY: Das Wiederherstellungsverfahren ist fehlgeschlagen.

Tabelle 3-5 Durch das Leucht- und Blinkverhalten der LEDs dargestellte Systemzustände

PF1 (grün)	PF2 (grün)	PF3 (grün)	PF4 (grün)	PF5 (ERR) (rot)	FAIL (FAULT) (rot)	Beschreibung des Systemzustands
ON (2 sec) Herz-schlag						RECOVERY: Das Wiederherstellungsverfahren war erfolgreich.
Flash-Prozedure						
ON					ON	FLASH-PROZEDUR: Die Flash-Prozedur wurde gestartet. Bitte warten.
Running light	Running light	Running light			ON	FLASH-PROZEDUR: Die Flash-Prozedur wird ausgeführt.
Blink 50/800	Blink 50/800	Blink 50/800			ON	FLASH-PROZEDUR: Die Flash-Prozedur war erfolgreich.
				ON		FLASH-PROZEDUR: Die Flash-Prozedur ist fehlgeschlagen.
				Blink 50/100 (5 sec)		FLASH-PROZEDUR WARNUNG: Austausch des Rettungssystems. Schalten Sie das Gerät nicht aus. Wenn das Blinken aufhört, ist der Austausch des Rettungssystems beendet.
				ON		FLASH-PROZEDUR: Die DHCP/BOOTP-Anforderungen sind fehlgeschlagen.
				ON		FLASH-PROZEDUR: Das Einbinden (Mounten) des Datenspeichers (data storage device) ist fehlgeschlagen.
				ON		FLASH-PROZEDUR: Das Löschen der Dateisystem-Partition ist fehlgeschlagen.
				ON		FLASH-PROZEDUR: Das Laden des Firmware-Images ist fehlgeschlagen.
				ON		FLASH-PROZEDUR: Die Signatur des Firmware-Images ist ungültig.
				ON		FLASH-PROZEDUR: Das Installationsskript konnte nicht geladen werden.
				ON		FLASH-PROZEDUR: Die Signatur des Installationsskripts ist ungültig.
				ON		FLASH-PROZEDUR: Das Rollout-Skript ist fehlgeschlagen.

3.3 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.

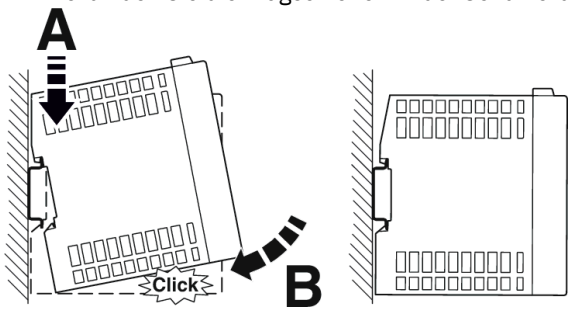


Bild 3-9 Aufrasten des Geräts auf eine Tragschiene

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**).

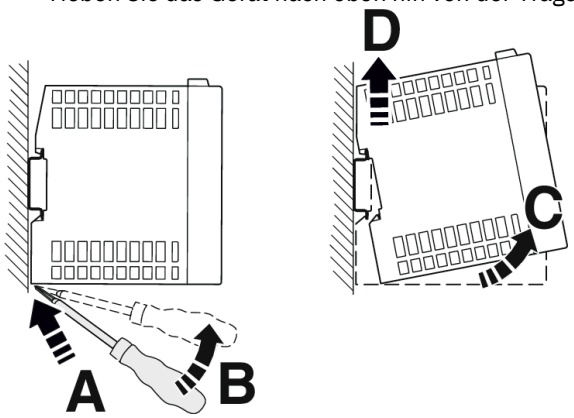


Bild 3-10 Demontage des Geräts

3.3.1 Leiter wählen

Die Geräte werden mit eine Push-in-Steckern (COMBICON-Steckverbindungen) ausgeliefert. Beachten Sie die Vorgaben an verwendbare Leiter sowie an die Aderendhülsen:

Tabelle 3-6 Auswahl der Leiter/Aderendhülse/Schraubendreher

Leiter	Push-in	Schraube
Leiterquerschnitt starr min.	0,14 mm^2	
Leiterquerschnitt starr max.	1,5 mm^2	
Leiterquerschnitt flexibel min.	0,14 mm^2	
Leiterquerschnitt flexibel max.	1,5 mm^2	
Leiterquerschnitt flexibel mit Aderendhülse ohne Kunststoffhülse min.	0,25 mm^2	
Leiterquerschnitt flexibel mit Aderendhülse ohne Kunststoffhülse max.	1,5 mm^2	
Leiterquerschnitt flexibel mit Aderendhülse mit Kunststoffhülse min.	0,25 mm^2	
Leiterquerschnitt flexibel mit Aderendhülse mit Kunststoffhülse max.	0,75 mm^2	0,5 mm^2
Verwendbare Aderendhülse ohne Kunststoffhülse: max. Leiterquerschnitt	1,5 mm^2	
Verwendbare Aderendhülse ohne Kunststoffhülse: max. Leiterquerschnitt	0,75 mm^2 (nach DIN 46228 Farbcode grau)	0,5 mm^2 (nach DIN 46228 Farbcode weiß)
Leiterquerschnitt AWG min.	24	
Leiterquerschnitt AWG max.	16	
Abisolierlänge	9 mm	

Tabelle 3-7 Angaben zu Aderendhülsen

Empfohlene Crimpzange	1212034 CRIMPFOX 6	
Aderendhülsen ohne Isolierkragen, nach DIN 46228-1	Querschnitt: 0,25 mm^2;	Länge: 7 mm
	Querschnitt: 0,34 mm^2;	Länge: 7 mm
	Querschnitt: 0,5 mm^2;	Länge: 8 mm ... 10 mm
	Querschnitt: 0,75 mm^2;	Länge: 8 mm ... 10 mm
	Querschnitt: 1 mm^2;	Länge: 8 mm ... 10 mm
	Querschnitt: 1,5 mm^2;	Länge: 10 mm

3.4 Versorgungsspannung anschließen

ACHTUNG: Elektrische Spannung
Das Modul ist ausschließlich für den Betrieb mit Sicherheitskleinspannung (SELV/PELV) ausgelegt. Im redundanten Betrieb müssen beide Spannungsversorgungen den Anforderungen der Sicherheitskleinspannung genügen. Sehen Sie eine Überstromschutzeinrichtung (I ≤ 5 A) in der Installation vor.

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

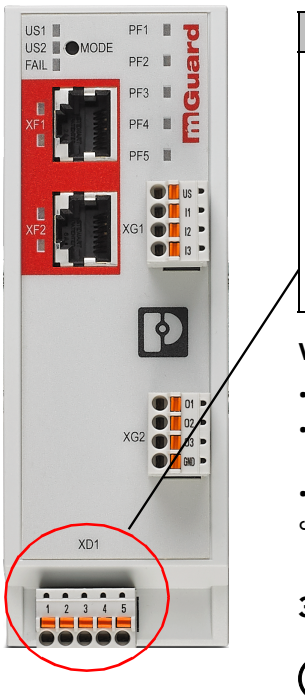


Tabelle 3-8 Spannungsversorgung über COMBICON-Steckverbindung

COMBICON	1	2	3	4	5
XD1	US1	GND	US2	GND	Funktionserde
			(FL MGUARD 4302/4305)		⏚
1 2 3 4 5 US1 GND US2 GND FE	12...36 V	0 V	12...36 V	0 V	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 3-8).
- Stecken Sie die COMBICON-Steckverbindung **XD1** auf das Gerät.

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

3.4.1 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**.

3.5 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.

3.5.1 Verwendung von RJ45-Ethernet-Steckern

Tabelle 3-9 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 3-9).
- 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.

3.6 Schalteingänge/Schaltausgänge (I/Os)

3.6.1 I/Os anschließen

ACHTUNG: 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.

Alternative Bezeichnung der I/Os im WBM: „**CMD**“ = „**I**“ und „**ACK**“ = „**O**“ .

Zwischen die Servicekontakte **US** und **I** (**1–3**) kann ein Taster oder ein Ein-/Aus-Schalter (z. B. Schlüsselschalter) angeschlossen werden (siehe Tabelle 3-10).

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.

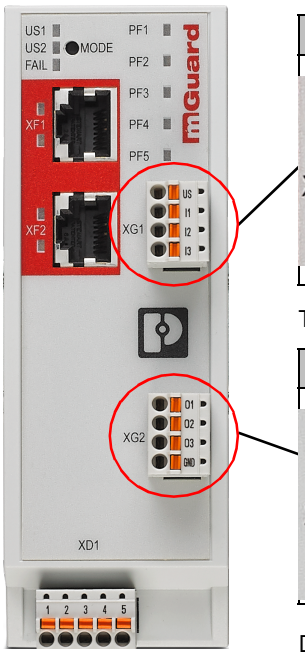


Tabelle 3-10 **Eingang I1–3**: Servicekontakte über COMBICON-Steckverbindung

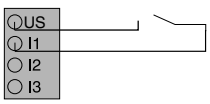
COMBICON XG1	Eingang (I1–3)		Beispiel
	**US**	Spannungsausgang (**US**) (+) (Kurzschlussfest)	
	I1	Schalteingänge **(I1–3)**	
	I2		
	I3		

Tabelle 3-11 **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 12 ... 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 3-10 und 3-11).
- Stecken Sie die COMBICON-Steckverbindung **XG1** bzw. **XG2** auf das Gerät.

3.7 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.

Stellen Sie sicher, dass Unbefugte keinen Zugriff auf die SD-Karte haben.

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

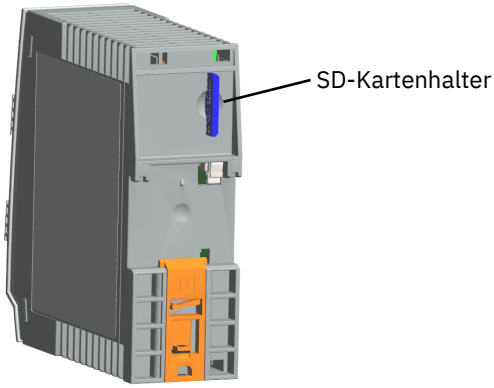


Bild 3-11 SD-Kartenhalter auf der Rückseite des Geräts

4 FL MGUARD 4102 PCI(E)

Tabelle 4-1 Aktuell verfügbare Produkte

Produktbezeichnung	Artikelnummer
FL MGUARD 4102 PCI	1441187
FL MGUARD 4102 PCIE	1357842

Produktbeschreibung

Die Geräte der **FL MGUARD 4000-Serie** sind Security-Router mit intelligenter Stateful-Packet-Inspection-Firewall und integriertem IPsec-VPN und OpenVPN mit bis zu 250 VPN-Tunneln.

Der FL MGUARD 4102 PCI(E) hat die Form einer PCI-kompatiblen Steckkarte. Es gibt ihn in zwei Ausführungen:

– **FL MGUARD 4102 PCI** für Geräte oder Maschinen mit PCI-Bus
– **FL MGUARD 4102 PCIE** für Geräte oder Maschinen mit PCI-Express-Bus

In diesem Handbuch wird zur Vereinfachung die Bezeichnung FL MGUARD 4102 PCI(E) für beide Ausführungen verwendet.

Bild 4-1 FL MGUARD 4102 PCI(E)

4.1 Gerätebeschreibung

Das Gerät verfügt über folgende Netzwerkanschlüsse:

– **Netzwerkinterface XF1 / WAN**: Ethernet 10/100/1000 Mbit/s (RJ45-Port)
– **Netzwerkinterface XF2 / LAN**: Ethernet 10/100/1000 Mbit/s (RJ45-Port)

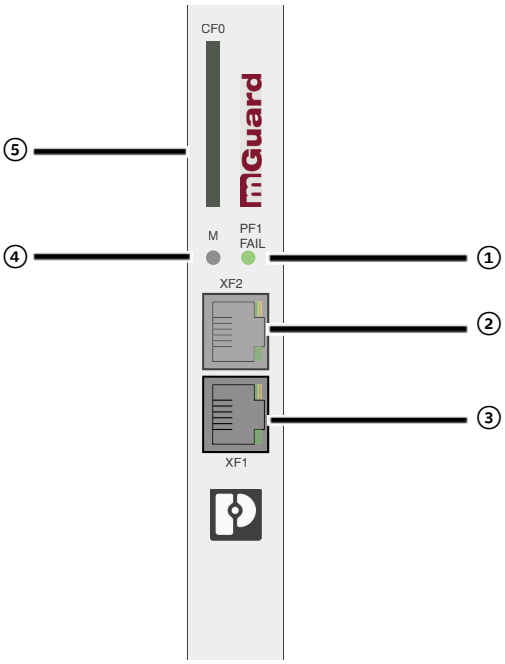


Bild 4-2 FL MGUARD 4102 PCI(E): Bedienelemente und Anzeigen

① Status- und Diagnose-LED „PF1“ / „FAIL“
(siehe Kapitel 4.2.2)

② Netzwerkinterface XF2/**LAN** (RJ45-Ethernet-Port) (siehe Kapitel 4.4)
LED SPD (oben)
LED LNK/ACT (unten) (siehe Kapitel 4.2.1)

③ Netzwerkinterface XF1/**WAN** (RJ45-Ethernet-Port) (siehe Kapitel 4.4)
LED SPD (oben)
LED LNK/ACT (unten)
(siehe Kapitel 4.2.1)

④ Mode-Taste
(siehe Kapitel 6)

⑤ SD-Kartenhalter (siehe Kapitel 4.5)

4.2 LED – Status- und Diagnoseanzeige

Mithilfe der Status- und Diagnose-LEDs werden unterschiedliche System- und Fehlerzustände des Geräts angezeigt (siehe Tabelle 4-2 und 4-3).

4.2.1 SPD und LNK/ACT

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

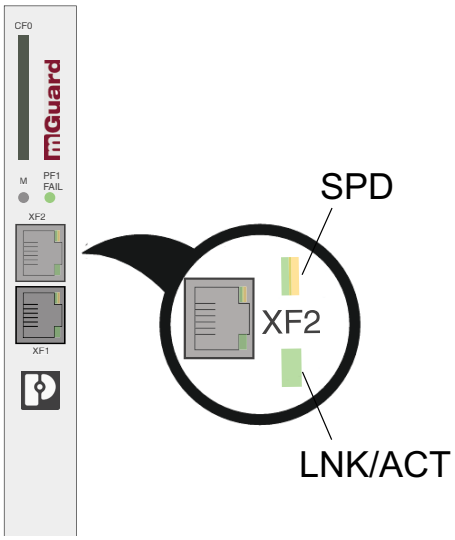


Bild 4-3 LED: SPD und LNK/ACT

Tabelle 4-2 LED: SPD und LNK/ACT

Bezeichnung	Farbe	Status	Bedeutung
SPD (XF1/2)	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) **oder** Inaktiv - keine Datenübertragung (wenn LED LNK/ACT nicht aktiv)
LNK/ACT (XF1/2)	Grün	An	Link aktiv
		Blinken	Datenpakete werden übertragen
		Aus	Link nicht aktiv
SPD und LNK/ACT	Diverse LED-Leuchtcodes	**Rescue-Prozedur / Flashen der Firmware** Siehe Kapitel 6.3, „Flashen der Firmware (Rescue Mode)“.	

4.2.2 PF1/FAIL

Die LED PF1/FAIL zeigt verschiedene Status und Fehlerzustände des Geräts an.

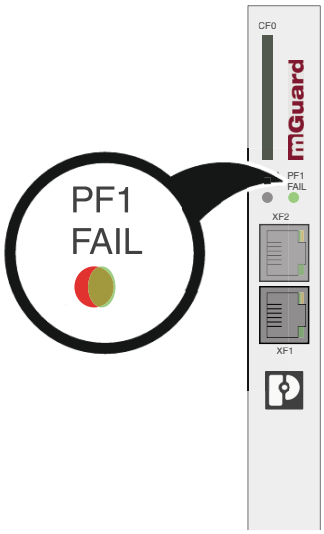


Bild 4-4 LED: PF1/FAIL

Tabelle 4-3 LED: PF1/FAIL

Bezeichnung	Farbe	Status	Bedeutung
PF1/FAIL	Rot/Grün	Blinkt	**Bootprozess.** Nach Anschluss des Gerätes an die Stromversorgungsquelle. Nach einigen Sekunden wechselt diese Anzeige zu Heartbeat.
	Grün	Blinkt	**Herzschlag**. Das Gerät ist korrekt angeschlossen und funktionsfähig.
	Rot	An	**Systemfehler**. Führen Sie einen Neustart durch. • Dazu die Mode-Taste kurz (ca. 5 Sekunden) drücken. • Alternativ: das Gerät kurz von der Stromversorgung trennen und wieder anschließen. Falls der Fehler weiterhin auftritt, starten Sie die Rescue-Prozedur (Flashen) (siehe Kapitel 6, „Smart-Mode“) oder wenden Sie sich an Ihre Bezugsquelle.

4.3 Montieren und demontieren

4.3.1 Sicherheitshinweise

Um den ordnungsgemäßen Betrieb sicherzustellen und die Sicherheit der Umgebung und von Personen zu gewährleisten, muss das Gerät richtig installiert, betrieben und gewartet werden.

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

ACHTUNG: Elektrostatische Entladung
Berühren Sie vor dem Einbau den freien Metallrahmen des PCs, in den Sie das Gerät einbauen möchten, um Ihren Körper elektrostatisch zu entladen.

Das Gerät enthält Bauelemente, die durch elektrostatische Entladung beschädigt oder zerstört werden können. Beachten Sie beim Umgang mit dem Gerät die notwendigen Sicherheitsmaßnahmen gegen elektrostatische Entladung (ESD) nach EN 61340-5-1 und IEC 61340-5-2.

ACHTUNG: Berührungsgefährliche Stromkreise
Die sichere Trennung von berührungsgefährlichen Stromkreisen ist nur gewährleistet, wenn die angeschlossenen Geräte die Anforderungen der VDE 0106-101 (Sichere Trennung) erfüllen. Für die sichere Trennung sind die Zuleitungen getrennt von berührungsgefährlichen Stromkreisen zu führen oder zusätzlich zu isolieren.

ACHTUNG: Funktstörungen
Dies ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funkstörungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen durchzuführen.

4.3.2 Gerät montieren

Bauen Sie das Gerät in einen freien PCI- oder PCI-Express-Steckplatz ein (PCI: 3,3 V und 5 V | PCIE: 3,3 V und 12 V) . Beachten Sie dabei die Hinweise in der Dokumentation zu Ihrem System.

4.4 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.

4.4.1 Verwendung von RJ45-Ethernet-Steckern

Tabelle 4-4 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 4-4).
- 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.

4.5 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.

Stellen Sie sicher, dass Unbefugte keinen Zugriff auf die SD-Karte haben.

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

Der SD-Kartenhalter befindet sich auf der Vorderseite des Geräts (siehe Kapitel 4.1).

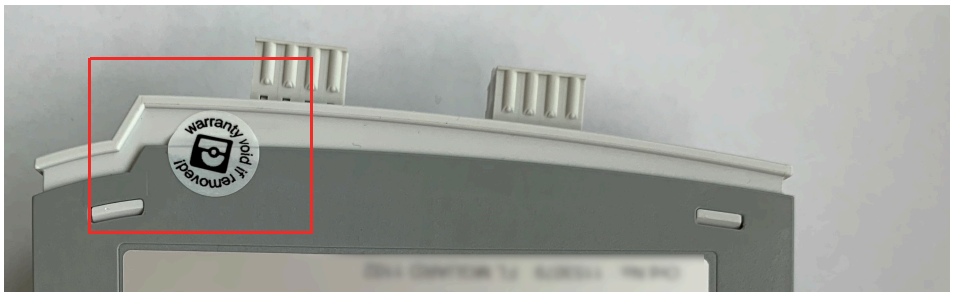
Technische Voraussetzung SD-Karte:

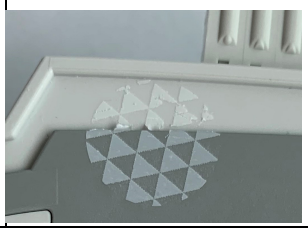
– SD- und SDHC-Karten bis max. 8 GB
– VFAT-kompatibles Dateisystem

5 Erstinbetriebnahme

Die Erstinbetriebnahme des Geräts erfolgt im Router-Modus.

Um Manipulationen am gelieferten Gerät zu verhindern und ein unbefugtes Öffnen des Gerätes zu erkennen, wurde am Gehäuse von Hutschienengeräten und auf der Verpackung von PCI-Karten ein Sicherheitssiegel angebracht.
Prüfen Sie vor der Erstinbetriebnahme, ob das Siegel intakt ist. Im Falle einer Entfernung/Beschädigung des Siegels würden Teile des Siegels auf dem Gehäuse/der Verpackung verbleiben.



Intakt	Beschädigt (teilweise)	Entfernt
		

Router-Modus (siehe Kapitel 5.3)

- 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 des internen LAN-Netzwerks (XF2-4 bzw. XF2-5) können ihre IP-Konfiguration automatisch per DHCP vom Gerät erhalten.
- Die Firewall des Geräts schützt automatisch alle über die LAN-Ports angeschlossenen Geräte vor externen Netzwerkzugriffen aus dem externen WAN-Netzwerks (XF1).
- Erwünschte externe Zugriffe auf die geschützten Geräte können gezielt erlaubt werden (Firewall- und NAT-Regeln).
- Die geschützten Geräte im LAN-Netzwerk können grundsätzlich auf alle Geräte in beiden Netzwerken zugreifen.
- Die geschützten Geräte im LAN-Netzwerk können auf Server-Dienste des Geräts zugreifen (HTTPS (WBM), SSH, DHCP, DNS).

5.1 Erforderliche Komponenten

- Netzwerkkabel (Ethernet)
- 24V-Stromversorgung (nur Tragschienengeräte)

5.2 Anschlussvoraussetzungen

5.2.1 Lokale Konfiguration über den LAN-Port

Der Konfigurationsrechner, mit dem Sie die Konfiguration vornehmen, muss an einen LAN-Port (XF2-4 bzw. XF2-5) des Geräts angeschlossen werden (siehe auch Kapitel 5.3).

5.2.2 Fernkonfiguration über den WAN-Port

Eine initiale Fernkonfiguration über den WAN-Port (HTTPS oder SSH) ist nicht möglich, da dies durch die voreingestellten Firewall-Regeln verhindert wird (siehe auch Kapitel 5.4).

5.3 Das Gerät wird bei der Erstinbetriebnahme im „Router-Modus“ (DHCP) betrieben

Im Router-Modus arbeitet das Gerät als Gateway zwischen verschiedenen Subnetzen (siehe Bild 5-1).

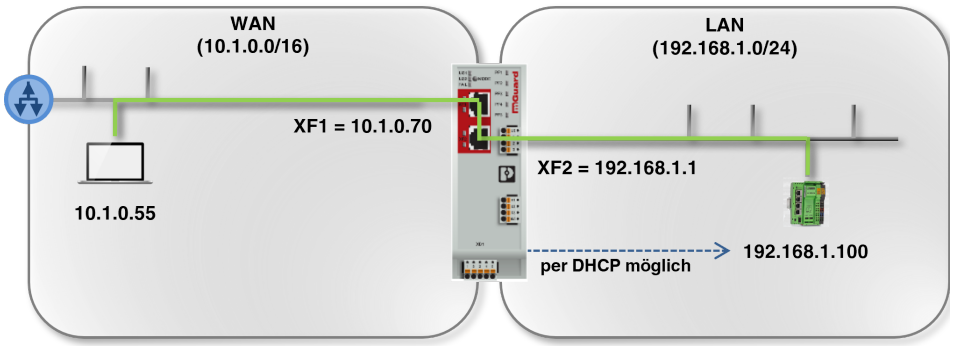


Bild 5-1 Gerät im Router-Modus betreiben (Beispielkonfiguration)

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

In den Werkseinstellungen wird dabei der Datenverkehr in der Richtung WAN nach LAN durch die Firewall blockiert.

Grundsätzlich können Clients in einem Netzwerk jedoch untereinander sowie mit Clients eines anderen Netzwerkes 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 Netzwerken ermöglicht werden.

5.3.1 Gerät starten

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

- Verbinden Sie das Gerät mit einer externen Spannungsversorgung (siehe Kapitel 3.4, „Versorgungsspannung anschließen“).

↪ Die LED FAIL leuchtet kurz rot.

↪ Während des Bootvorgangs leuchtet die LED PF5 rot.

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

↪ **PCI-Karten**: Die Betriebsbereitschaft des Geräts wird erreicht, wenn die LED PF1 grün blinkt (Herzschlag).

5.3.2 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 5-2).

Im Folgenden wird die Konfiguration des Geräts über das LAN-Interface (z. B. XF2) beschrieben. (Die Konfiguration über das WAN-Interface ist in den Werkseinstellungen nicht möglich.)

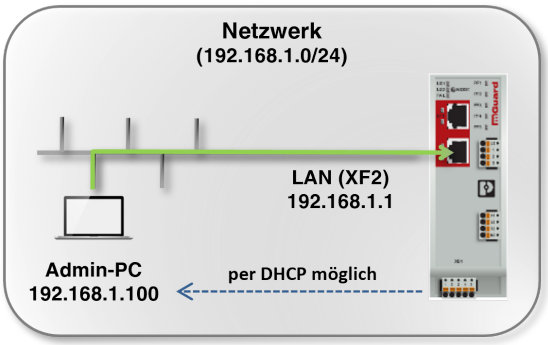


Bild 5-2 Netzwerkverbindung zum Gerät herstellen (Beispiel)

Voraussetzung

Das Gerät und der Konfigurationsrechner (Admin-PC) müssen sich im gleichen Subnetz befinden. Eine beispielhafte Netzwerkkonfiguration ist in Tabelle 5-1 angegeben.

Tabelle 5-1 IP-Konfiguration (Beispiel): Netzwerkverbindung herstellen

Gerät	IP	Netzmaske	Gateway
Gerät (Werkseinstellung für XF2)	192.168.1.1	24 (255.255.255.0)	-
Konfigurationsrechner (**Beispiel:** 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 (z. B. XF2) des LAN-Interface des Geräts (siehe Bild 5-2).
- 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 das LAN-Interface (XF2) automatisch eine IP-Konfiguration zu (z. B. 192.168.1.100/24).

IP-Konfiguration prüfen

- Öffnen Sie z. B. 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 (Windows 10)

Um die IP-Einstellung des Konfigurationsrechners automatisch zu beziehen, gehen Sie wie folgt vor (Beispiel: Microsoft Windows):

- 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)*“.

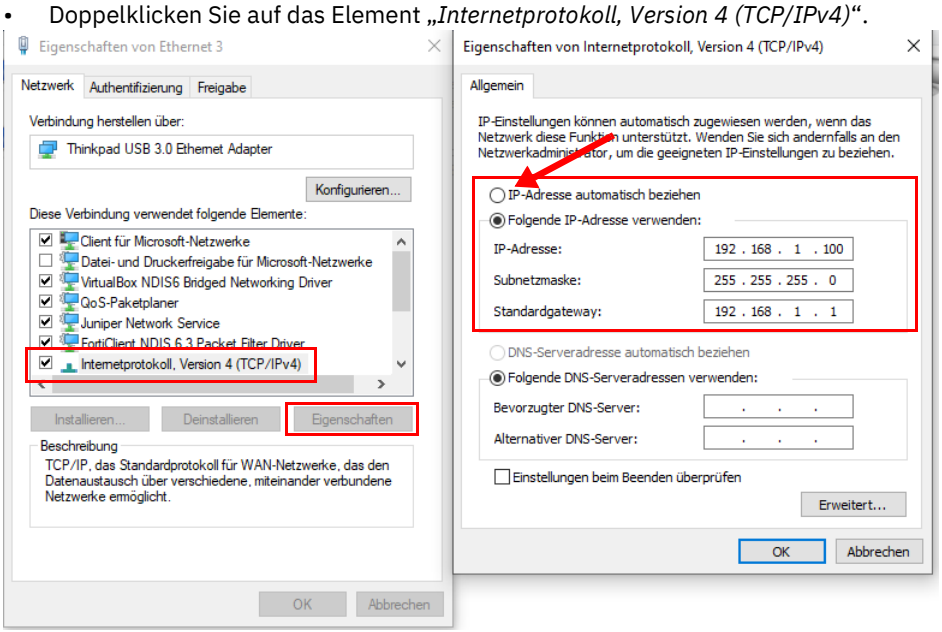


Bild 5-3 IP-Einstellung des Konfigurationsrechners (Admin-PC) ändern

- 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 5-3 / Tabelle 5-1 ein.
- Bestätigen Sie mit „*OK*“

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

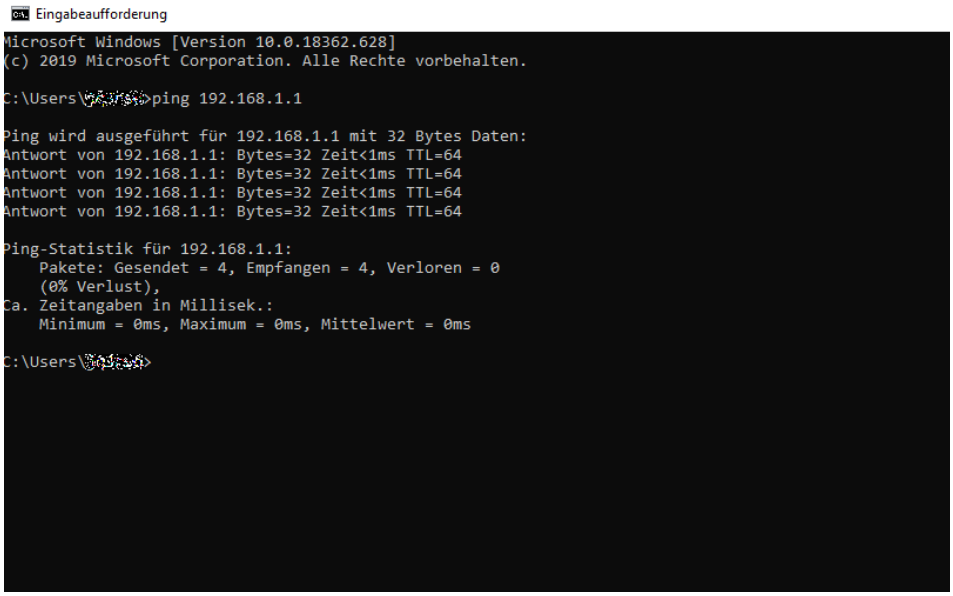
↪ Das Gerät dient dem Konfigurationsrechner als Standard-Gateway.

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.



5.3.3 IP-Adresse per BootP zuweisen

Nach der Zuweisung einer IP-Adresse per BootP steht die IP-Adresse 192.168.1.1 nicht länger als Zugriffsmöglichkeit zur Verfügung.

Für die IP-Adressvergabe nutzt das Gerät das BootP-Protokoll. Sie können die IP-Adresse auch über BootP zuweisen. Das Internet stellt eine Vielzahl von BootP-Servern zur Verfügung. Sie können ein beliebiges dieser Programme für die Adressvergabe nutzen.

Hinweise zu BootP

Bei der ersten Inbetriebnahme sendet das Gerät ununterbrochen bis zum Erhalt einer gültigen IP-Adresse BootP-Requests aus. Sobald das Gerät eine korrekte IP-Adresse erhält, werden keine weiteren BootP-Requests gesendet. Danach steht die IP-Adresse 192.168.1.1 nicht länger als Zugriffsmöglichkeit zur Verfügung.

Nachdem das Gerät eine BootP-Antwort erhalten hat, sendet er keine BootP-Anfragen aus, auch nicht nach einem Neustart. Damit das Gerät erneut BootP-Requests sendet, muss entweder die Werkseinstellung wiederhergestellt oder eine der Prozeduren (Recovery oder Flash/Rescue) ausgeführt werden.

5.3.4 Wenn Sie nicht zur Administrator-Webseite des Geräts gelangen

Falls Sie die konfigurierte Adresse vergessen haben

Falls Sie die aktuelle Adresse nicht kennen, können Sie beim Gerät die **Recovery**-Prozedur ausführen, sodass die oben angegebenen Werkseinstellungen der IP-Adresse wieder in Kraft treten (siehe Kapitel 6.2).

Falls die Administrator-Webseite nicht angezeigt wird

Wenn auch nach wiederholtem Versuch der Web-Browser meldet, dass die Seite nicht angezeigt werden kann, versuchen Sie Folgendes:

- Deaktivieren Sie gegebenenfalls bestehende Firewalls.
- Achten Sie darauf, dass der Browser keinen Proxy-Server verwendet.
- Falls andere LAN-Verbindungen auf dem Rechner aktiv sind, deaktivieren Sie diese für die Zeit der Konfiguration.

Bei erfolgreichem Verbindungsaufbau

Nach erfolgreicher Verbindungsaufnahme erscheint evtl. ein Sicherheitshinweis:

Da das Gerät nur über verschlüsselte Zugänge administrierbar ist, wird es mit einem selbstunterzeichneten Zertifikat ausgeliefert:

- Quittieren Sie entsprechende Sicherheitshinweise mit „Ja“, „OK“, „Weiter“ etc.

↪ Das Login-Fenster wird angezeigt.

Bild 5-4 Login

- Geben Sie den voreingestellten Benutzernamen und das voreingestellte Passwort ein, um sich einzuloggen (Groß- und Kleinschreibung beachten):

Benutzername:	admin	root
Passwort:	mGuard	root

Die Anzahl gleichzeitiger Web-Sitzungen (HTTPS) ist für die Benutzer *root*, *admin*, *netadmin* und *audit* auf 10 begrenzt.

Anschließend können Sie das Gerät über die Web-Oberfläche konfigurieren. Informationen dazu finden Sie im Benutzerhandbuch UM DE FW MGUARD10 „Web-based Management“ im Phoenix Contact Web Shop unter phoenixcontact.net/product/1357828.

Ändern Sie aus Sicherheitsgründen bei der ersten Konfiguration die Root- und Administrator-Passwörter.

5.4 Fernkonfiguration

Standardmäßig ist die Möglichkeit zur Fernkonfiguration deaktiviert und durch die Einstellungen der Firewall blockiert.

Die Aktivierung des Fernzugangs erfolgt unter **Verwaltung >> Systemeinstellungen >> Shell-Zugang** bzw. **Verwaltung >> Web-Einstellungen >> Zugriff**.

Voraussetzung

Das Gerät muss so konfiguriert sein, dass es eine Fernkonfiguration zulässt.

Schalten Sie die Möglichkeit des Fernzugangs unter **Verwaltung >> Systemeinstellungen >> Shell-Zugang**„bzw. **Verwaltung >> Web-Einstellungen >> Zugriff**“ ein. Konfigurieren Sie an dieser Stelle ebenfalls die „Erlaubten Netzwerke“.

Vorgehensweise

Um von einem entfernten Rechner aus das Gerät über seine Web-Oberfläche zu konfigurieren, stellen Sie von dort die Verbindung zum Gerät her.

Gehen Sie wie folgt vor:

- Starten Sie dazu auf dem entfernten Rechner den Web-Browser.
- Als Adresse geben Sie die IP-Adresse an, unter der das Gerät von extern über das Internet bzw. den WAN-Port (XF1) erreichbar ist und gegebenenfalls zusätzlich die Port-Nummer.

Beispiel

Wenn das Gerät beispielsweise über die Adresse https://123.45.67.89 über das Internet zu erreichen ist und für den Fernzugang die Port-Nummer 443 festgelegt ist, dann muss bei der entfernten Gegenstelle im Web-Browser folgende Adresse angegeben werden: https://123.45.67.89/

Bei einer anderen Port-Nummer müssen Sie die Port-Nummer hinter der IP-Adresse angeben, z. B.: https://123.45.67.89:442/

Konfiguration

Anschließend können Sie das Gerät über die Web-Oberfläche konfigurieren. Informationen dazu finden Sie im Benutzerhandbuch UM DE FW MGU-ARD10 „Web-based Management“ im Phoenix Contact Web Shop unter phoenixcontact.net/product/1357828.

5.4.1 Netzwerk-Clients schützen

- Verbinden Sie die zu schützenden Geräte über einen LAN-Netzwerkport (**XF2-4** bzw. **XF2-5**) mit **dem internen Netzwerk (LAN)** des Geräts.
  (Um weitere Geräte zu schützen, verbinden Sie diese über einen zusätzlichen Switch mit dem Gerät.)
- Verbinden Sie das umgebende Netzwerk über einen Switch über den Netzwerkport (**XF1**) mit **dem externen Netzwerk (WAN)**.

↪ Alle Netzwerkpakete WAN --> LAN werden verworfen.

↪ Alle Netzwerkpakete LAN --> WAN werden angenommen und weitergeleitet.

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

Um ein Gerät mit einer gespeicherten Konfiguration von SD-Karte in Betrieb zu nehmen, können Sie Konfigurationsprofile über das WBM speichern und wiederherstellen (siehe Benutzerhandbuch UM DE FW MGUARD10 „Web-based Management“ im Phoenix Contact Web Shop unter phoenixcontact.net/product/1357828).

5.6 Web-based Management verwenden

5.6.1 Unterstützte Webbrowser

Unterstützt werden folgende Webbrowser in ihrer jeweils aktuellen Version:

– *Mozilla Firefox, Google Chrome, Microsoft Edge*

5.6.2 Unterstützte Benutzer

Die Benutzer *admin* und *root* können sich auf dem Gerät anmelden (alle verfügbaren Interfaces). Sie haben einen funktional uneingeschränkten Zugriff auf das Gerät. Die Anzahl gleichzeitiger Web-Sitzungen (HTTPS) ist auf 10 begrenzt. Die Anzahl gleichzeitiger SSH-Anmeldungen (SSH-Sitzungen) kann konfiguriert werden.

5.6.3 Beim Gerät anmelden

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

- Verbinden Sie den Konfigurationsrechner mit dem Gerät (siehe Kapitel 5.2).
- 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.

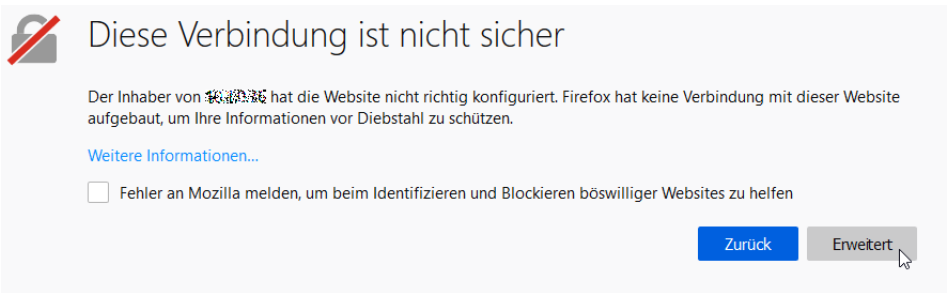


Bild 5-5 Zertifikatswarnung (Firefox)

- 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 5-6 Anmeldeseite des Web-based Managements

- Melden Sie sich mit dem Benutzernamen *admin* oder *root* und dem zugehörigen Administrator-Passwort (Werkseinstellungen: *mGuard* bzw. *root*) an.

↪ Die Startseite des Web-based Managements wird geöffnet.

Die Anzahl gleichzeitiger Web-Sitzungen (HTTPS) ist für die Benutzer *root*, *admin*, *netadmin* und *audit* auf 10 begrenzt.

Die Funktionen, die mittels Web-based Management konfiguriert werden können, werden im Benutzerhandbuch UM DE FW MGUARD10 „Web-based Management“ im Phoenix Contact Web Shop unter phoenixcontact.net/product/1357828 beschrieben.

5.7 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 (ca. 5 Sekunden).
– Möglichkeit 2: Unterbrechen Sie die kurzzeitig die Spannungsversorgung.
– Möglichkeit 3: Starten Sie das Gerät über das WBM neu.

5.8 Generic Administration Interface (GAI) verwenden

Um das Gerät mittels GAI zu konfigurieren oder Informationen vom Gerät abzurufen, müssen Sie sich zunächst per SSH-Verbindung am Gerät anmelden.

Die Konfiguration des Geräts via *Generic Administration Interface* (GAI) wird im Anwenderhandbuch UM DE GAICONFIG MGUARD10 beschrieben (erhältlich z. B. unter phoenixcontact.net/product/1357828).

6 Smart-Mode

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

– „Neustart“
– „Wiederherstellen des Konfigurationszugriffs (Recovery Mode)“
– „Flashen der Firmware (Rescue Mode)“
– „Das Gerät außer Betrieb nehmen (Decommissioning Mode)“

6.1 Neustart

ACHTUNG: Alle nicht gespeicherten Änderungen gehen verloren.

Anwendungsfall

Das betriebsbereite Gerät soll mit den konfigurierten Einstellungen neu gestartet werden.

Ergebnis

– Das Gerät wird neu gestartet.

Durchführung (Tragschienen-Geräte)

• Halten Sie die Mode-Taste ca. 3 Sekunden gedrückt, bis die **LED „PF5“** rot leuchtet.
• Lassen Sie die Mode-Taste los.
↳ Das Gerät wird neu gestartet.

Durchführung (PCI-Karten)

• Halten Sie die Mode-Taste ca. 3 Sekunden gedrückt.
• Lassen Sie die Mode-Taste los.
↳ Das Gerät wird neu gestartet.

6.2 Wiederherstellen des Konfigurationszugriffs (Recovery Mode)

Passwörter bleiben erhalten und werden nicht auf Werkseinstellungen zurückgesetzt.

Anwendungsfälle

– Die IP-Konfiguration des Geräts ist nicht bekannt. Es ist deshalb nicht mehr möglich, auf das Gerät zuzugreifen.
– Die Konfiguration des Geräts (Admin- und Root-Passwörter ausgenommen) soll auf Werkseinstellungen zurückgesetzt werden. Die aktuelle Konfiguration soll dabei als Konfigurationsprofil für eine optionale Wiederherstellung erhalten bleiben.

Ergebnis

– Das Gerät wird auf Werkseinstellungen zurückgesetzt (Admin- und Root-Passwörter ausgenommen).
– Vor der Durchführung der Recovery-Prozedur wird die aktuelle Konfiguration des Geräts in einem neu erstellten Konfigurationsprofil gespeichert („Recovery-DATUM“).
– Der Zugriff auf das Gerät über die werkseitig voreingestellte IP-Adresse ist wieder möglich (siehe Kapitel 2.4):

Tabelle 6-1 Wiederhergestellte Werkseinstellungen (siehe Kapitel 2.4)

LAN-Interface (XF2-4 bzw. XF2-5) Management-IP	WAN-Interface (XF1)
192.168.1.1	Netzwerk-Modus: Router Router-Modus: DHCP Externe Anfragen an das WAN-Interface werden von der Firewall verworfen.

Durchführung (Tragschienen-Geräte)

• Drücken Sie die Mode-Taste 6-mal.
• Warten Sie ca. 2 Sekunden, bis die **LED PF1** grün leuchtet.
• Drücken Sie die Mode-Taste erneut 6-mal.
↳ Das Gerät wird auf Werkseinstellungen zurückgesetzt und neu gestartet.
↳ Das Gerät ist betriebsbereit, wenn die LED PF5 (rot) erloschen ist und die LED PF1 grün blinkt (Herzschlag).

Durchführung (PCI-Karten)

• Drücken Sie die Mode-Taste 6-mal.
• Warten Sie ca. 2 Sekunden, bis die **LED PF1** kurz grün leuchtet.
• Drücken Sie die Mode-Taste erneut 6-mal.
↳ Das Gerät wird auf Werkseinstellungen zurückgesetzt und neu gestartet.
↳ Bei Erfolg leuchtet die LED PF1 grün. Bei Misserfolg leuchtet die LED PF1 rot.
↳ Das Gerät ist betriebsbereit, wenn die LED PF1 grün blinkt (Herzschlag).

Das Konfigurationsprofil mit der Bezeichnung „Recovery-DATUM“) erscheint anschließend in der Liste der Konfigurationsprofile und kann bearbeitet und mit oder ohne Änderungen wiederhergestellt werden.

Wiederherstellung des gespeicherten Konfigurationsprofils

- Melden Sie sich nach Abschluss der Recovery-Prozedur auf der Weboberfläche des Geräts an.
- Öffnen Sie das Menü **Verwaltung >> Konfigurationsprofile**.
- Wählen Sie das bei der Recovery-Prozedur erstellte Konfigurationsprofil mit dem Namen „Recovery-DATUM“ (z. B. „Recovery-2022.04.01-18:02:50“).
- Klicken Sie auf das Icon „Profil bearbeiten“, um das Konfigurationsprofil zu analysieren und anschließend mit oder ohne Änderungen wiederherzustellen.
- Klicken Sie auf das Icon „Übernehmen“, um die Änderungen zu übernehmen.

6.3 Flashen der Firmware (Rescue Mode)

Anwendungsfälle

- Eine neue Firmware-Version soll auf dem Gerät installiert werden.
- Das Administrator-Passwort ist nicht bekannt. Eine Anmeldung auf dem Gerät ist deshalb nicht mehr möglich.
- Das Gerät soll auf Werkseinstellungen zurückgesetzt werden.

Ergebnis

- Das Gerät wird mit der neuen Firmware-Version geflasht.
- Das Gerät wird auf Werkseinstellungen zurückgesetzt.

ACHTUNG: Das Flashen der Firmware löscht alle Passwörter und Konfigurationen auf dem Gerät. Das Gerät wird auf seine werkseitige Voreinstellung zurückgesetzt.

ACHTUNG: Ab einer installierten Firmware-Version mGuard 10.5.0 ist ein Downgrade auf eine niedrigere Firmware-Version nicht mehr möglich. Die LED PF5 leuchtet in diesem Fall rot, ein Neustart ist erforderlich.

Voraussetzungen

- Laden Sie die gewünschte Firmware-Version von der Webseite herunter: phoenixcontact.net/product <Bestellnummer>.
  - **Download-Datei:** z. B. *Firmware-mGuard-10.5.0.zip*
  - **Update-Dateien** (= entpackte Zip-Datei):
    firmware.img.aarch64.p7s
    install.aarch64.p7s

6.3.1 Flashen (Durchführung)

ACHTUNG: Spannungsversorgung nicht unterbrechen
Unterbrechen Sie während der Flash-Prozedur nicht die Spannungsversorgung. Das Gerät könnte beschädigt werden. Wenden Sie sich in diesem Fall an den Hersteller.

Beim Flashen wird die Firmware immer zuerst von einer SD-Karte geladen. Nur wenn keine SD-Karte gefunden wird, wird die Firmware von einem entsprechend konfigurierten TFTP-Server geladen.

Flash-Dateien herunterladen

- Öffnen Sie die Produkt-Webseite im Phoenix Contact Web Shop unter: phoenixcontact.com/products.
- Wählen Sie die Registerkarte *Downloads* und die Kategorie *Firmware-Update*.
- Laden Sie gewünschte **Download-Datei** herunter: z. B. *Firmware-mGuard-10.5.0.zip*
- Entpacken Sie die Zip-Datei.
- Kopieren Sie alle entpackten Dateien aus dem Verzeichnis *aarch64* (*firmware.img.aarch64.p7s, install.aarch64.p7s*)
  - in ein beliebiges Verzeichnis (z. B. */mGuard-Firmware*) auf dem TFTP-Server oder
  - in das Verzeichnis */Firmware* auf der SD-Karte.

Für Informationen zur Verwendung von SD-Karten siehe Kapitel 3.7 und 4.5.

FL MGUARD 2102/4302
FL MGUARD 2105/4305

Flash-Prozedur ausführen (Tragschienen-Geräte)

ACHTUNG: Ein vorzeitiger Neustart kann das Gerät beschädigen
Unterbrechen Sie nicht die Spannungsversorgung! Warten Sie unbedingt, bis die Flash-Prozedur vollständig abgeschlossen wurde (Dauer: ca. 2 Minuten).

Gehen Sie wie folgt vor:

- Halten Sie die Mode-Taste des Gerätes ca. 10 Sekunden gedrückt, bis alle PF-LEDs (PF1 – PF5) grün leuchten.
- Lassen Sie die Mode-Taste los. (Ansonsten wird das Gerät neu gestartet.)

↳ Die Flash-Prozedur wird gestartet.

↳ Nach ca. 20 Sekunden blinken die LEDs PF1, PF2 und PF3 im Modus „Lauflicht/Running light“ (grün). Die LED FAIL leuchtet (rot):
  - Zunächst wird nach einer eingelegten SD-Karte und dort im Verzeichnis Firmware nach den entsprechenden Update-Dateien gesucht.
  - Wird keine SD-Karte gefunden, sucht das Gerät über die LAN-Schnittstelle (XF2) nach einem DHCP-Server, um von diesem eine IP-Adresse zu beziehen.

↳ Die Dateien werden von SD-Karte oder von einem vorhandenen TFTP-Server geladen und installiert.

↳ Nach insgesamt ca. 60 Sekunden wird das Gerät automatisch neu gestartet.

↳ Nach dem Neustart leuchten die LEDs FAIL (rot) und PF1 (grün) permanent.

ACHTUNG: Schalten Sie das Gerät in diesem Zustand nicht vorzeitig aus.

ACHTUNG: Warten Sie, bis die Flash-Prozedur vollständig beendet wurde.

↳ Nach weiteren 60 Sekunden blinken die LEDs PF1, PF2 und PF3 gleichzeitig (grün).

↳ Die Flash-Prozedur wurde erfolgreich beendet.

- Starten Sie das Gerät neu, indem Sie kurz die Mode-Taste drücken oder das Gerät vorübergehenden von der Spannungsversorgung trennen.

↳ Das Gerät ist betriebsbereit, wenn die **LED PF1** grün blinkt (Herzschlag).

FL MGUARD 4102 PCI(E)

Flash-Prozedur ausführen (PCI-Karten)

ACHTUNG: Ein vorzeitiger Neustart kann das Gerät beschädigen
Unterbrechen Sie nicht die Spannungsversorgung! Warten Sie unbedingt, bis die Flash-Prozedur vollständig abgeschlossen wurde (Dauer: ca. 2 Minuten).

- Halten Sie die Mode-Taste an der Frontblende des Geräts ca. 10 Sekunden gedrückt, bis die **LED PF1** sowie die LEDs der **Ethernet-Buchsen (XF1/2)** grün leuchten.
- Lassen Sie die Mode-Taste los. (Ansonsten wird das Gerät neu gestartet.)

↳ Die Flash-Prozedur wird gestartet.

↳ Nach ca. 20 Sekunden blinken die LEDs PF1/FAIL und SPD (XF1/2) im Modus „Lauflicht/Running light“ (grün):

- Zunächst wird nach einer eingelegten SD-Karte und dort im Verzeichnis Firmware nach den entsprechenden Update-Dateien gesucht.
- Wird keine SD-Karte gefunden, sucht das Gerät über die LAN-Schnittstelle (XF2) nach einem DHCP-Server, um von diesem eine IP-Adresse zu beziehen.

↳ Die Dateien werden von SD-Karte oder einem vorhandenen TFTP-Server geladen und installiert.

↳ Nach insgesamt ca. 60 Sekunden wird das Gerät automatisch neu gestartet.

↳ Nach dem Neustart leuchtet die LED PF1/FAIL permanent (grün).

ACHTUNG: Schalten Sie das Gerät in diesem Zustand nicht vorzeitig aus.

ACHTUNG: Warten Sie, bis die Flash-Prozedur vollständig beendet wurde.

↳ Nach weiteren 60 Sekunden blinken die LEDs PF1/FAIL und SPD (XF1/2) gleichzeitig grün.

↳ Die Flash-Prozedur wurde erfolgreich beendet.

- Starten Sie das Gerät neu, indem Sie kurz die Mode-Taste drücken.

↳ Das Gerät ist betriebsbereit, wenn die LED PF1 grün blinkt (Herzschlag).

6.3.2 Konfigurationsprofil während Flash-Vorgang hochladen

Sie können ein erstelltes Konfigurationsprofil (ATV-Profil) während des Flash-Vorgangs automatisch auf das Gerät hochladen und aktivieren.

Das Blinkverhalten der LEDs nach dem Beenden des Flash-Vorgangs ist in diesem Fall abweichend vom Standardblinkverhalten.

Vorbereitung

Erstellen Sie die Datei *preconfig.sh* mit folgendem Inhalt. (Beachten Sie, dass die Datei im UNIX-Format erstellt werden muss.)

preconfig.sh: Für **unverschlüsselte** ATV-Profile

```
#!/bin/sh -ex
exec gaiconfig --factory default --silent --set-all < /bootstrap/preconfig.atv
```

preconfig.sh: Für **verschlüsselte** ATV-Profile (ab Firmware-Version mGuard 10.5.0)

```
#!/bin/sh -ex
/Packages/mguard-tpm2_0/mbin/tpm2_pkcs7 < /bootstrap/preconfig.atv.p7e > /bootstrap/preconf.atv
gaiconfig --factory-default --set-all < /bootstrap/preconf.atv
```

Wenn Sie ein mit dem Gerätezertifikat verschlüsseltes Konfigurationsprofil hochladen wollen, sollten Sie die Datei von **.atv* in **.atv.p7e* umbenennen. Verschlüsselte und unverschlüsselte Konfigurationsprofile können so leichter auseinandergehalten werden.

Das Gerät behandelt das ATV-Profil unabhängig von der Dateiendung gleich.

Während des Flash-Vorgangs sucht das Gerät nach folgenden Dateien und lädt sie hoch:

- */Rescue Config/<Seriennummer>.atv*
- */Rescue Config/<Seriennummer>.atv.p7e*
- */Rescue Config/preconfig.atv*
- */Rescue Config/preconfig.atv.p7e*
- */Rescue Config/preconfig.sh*

Konfigurationsprofil von SD-Karte laden

Um ein Konfigurationsprofil während des Flash-Vorgangs auf das Gerät hochzuladen und zu aktivieren, gehen Sie wie folgt vor:

1. Erstellen Sie auf der SD-Karte die Verzeichnisse *Firmware* und *Rescue Config.*
2. Benennen Sie das gespeicherte Konfigurationsprofil in *preconfig.atv oder <Seriennummer>.atv* um.
3. Kopieren Sie das Konfigurationsprofil in das Verzeichnis *Rescue Config*.
4. Kopieren Sie die Datei *preconfig.sh* (UNIX-Format) in das Verzeichnis *Rescue Config*.
5. Führen Sie den Flash-Vorgang wie für Ihr Gerät beschrieben durch.

Konfigurationsprofil vom TFTP-Server laden

Um ein Konfigurationsprofil während des Flash-Vorgangs von einem TFPT-Server zu laden und zu aktivieren, siehe Beschreibung im Kapitel 6.3.3.

6.3.3 Flashen (DHCP- und TFTP-Server einrichten)

ACHTUNG: Netzwerkprobleme
Falls Sie einen zweiten DHCP-Server in einem Netzwerk installieren, könnte dadurch die Konfiguration des gesamten Netzwerks beeinflusst werden.

ACHTUNG: Software von Drittanbietern
Phoenix Contact übernimmt keine Garantie oder Haftung bei der Verwendung von Produkten von Drittanbietern. Verweise auf Drittanbieter-Software stellen keine Empfehlung dar, sondern sind Beispiele für grundsätzlich verwendbare Programme.

Unter Windows

Falls Sie das Drittanbieter-Programm „*TFTPD32.exe*“ verwenden wollen, beschaffen Sie sich das Programm aus einer vertrauenswürdigen Quelle und gehen Sie wie folgt vor:

1. Wenn der Windows-Rechner an ein Netzwerk angeschlossen ist, trennen Sie ihn von diesem.
2. Erstellen Sie ein Verzeichnis auf dem Windows-Rechner, das Sie für den Flash-Vorgang von mGuard-Geräten verwenden wollen. Dieses Verzeichnis wird später als Root-Verzeichnis des TFTP-Servers ausgewählt. Während des Flash-Vorgangs werden alle benötigten Dateien aus diesem Verzeichnis geladen.
3. Kopieren Sie die gewünschten Firmware-Image-Datei(en) in das erstellte Verzeichnis.
4. Starten Sie das Programm *TFTPD32.exe*

   Die festzulegende Host-IP lautet: **192.168.10.1.** Das muss auch die Adresse für die Netzwerkkarte sein.
5. Klicken Sie die Schaltfläche **Browse**, um den Ordner auszuwählen, in dem die mGuard-Image-Dateien gespeichert sind: (z. B. *install.aarch64.p7s, firmware.img.aarch64.p7s*).

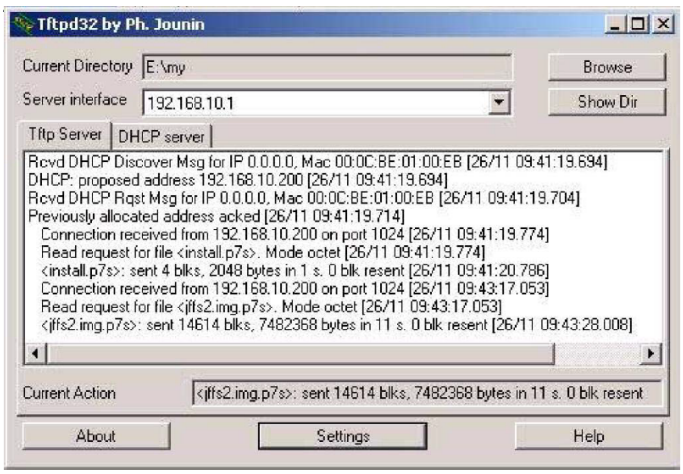
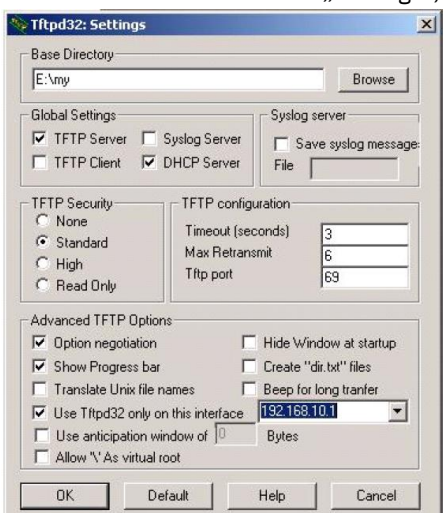


Bild 6-1 Host-IP eingeben

6. Wechseln Sie auf die Registerkarte „TFTP-Server“ bzw. „DHCP-Server“ und klicken Sie dann die Schaltfläche „Settings“, um die Parameter wie folgt zu setzen:



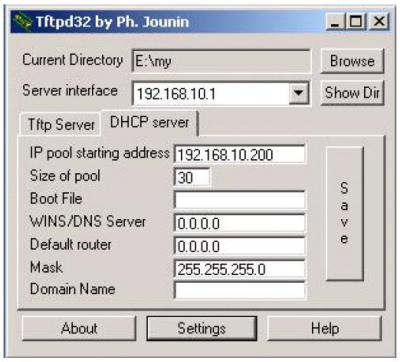


Bild 6-2 Settings

Unter Linux

Alle aktuellen Linux-Distributionen enthalten DHCP- und TFTP-Server.

1. Installieren Sie die entsprechenden Pakete nach der Anleitung der jeweiligen Distribution.
2. Konfigurieren Sie den DHCP-Server, indem Sie in der Datei */etc/dhcpd.conf* folgende Einstellungen vornehmen:

   subnet 192.168.134.0 netmask 255.255.255.0 {
   range 192.168.134.100 192.168.134.119;
   option routers 192.168.134.1;
   option subnet-mask 255.255.255.0;
   option broadcast-address 192.168.134.255;}
   Diese Beispiel-Konfiguration stellt 20 IP-Adressen (.100 bis .119) bereit. Es wird angenommen, dass der DHCP-Server die Adresse 192.168.134.1 hat (Einstellungen für ISC DHCP 2.0).

Der benötigte TFTP-Server wird in folgender Datei konfiguriert: */etc/inetd.conf*

3. Fügen Sie in diese Datei die entsprechende Zeile ein oder setzen Sie die notwendigen Parameter für den TFTP-Service. (Verzeichnis für Daten ist: */tftpboot*)

   tftp dgram udp wait root /usr/sbin/in.tftpd -s /tftpboot/

   Im Verzeichnis */tftpboot* müssen die mGuard-Imagedateien gespeichert sein: z. B. *install.aarch64.p7s, firmware.img.aarch64.p7s*.
4. Starten Sie dann den *inetd*-Prozess neu, um die Konfigurationsänderungen zu übernehmen.
5. Wenn Sie einen anderen Mechanismus verwenden, z. B. *xinetd*, dann informieren Sie sich in der entsprechenden Dokumentation.

6.3.3.1 TFTP-Server: Fehlermeldungen

Während des Flash-Vorgangs sucht das mGuard-Gerät standardmäßig nach den Dateien *rollout.sh, license.lic* und *<Seriennummer>.lic*. Sind diese Dateien nicht vorhanden, wird eine entsprechende Fehlermeldung angezeigt:

File rollout.sh: error 2 in system call CreateFile The system cannot find the file specified.

File <serial number>.lic : error 2 in system call CreateFile The system cannot find the file specified.

File licence.lic: error 2 in system call CreateFile The system cannot find the file specified.

Die Fehlermeldung kann ignoriert werden, wenn keine Lizenzdatei hochgeladen bzw. das Gerät nicht über das Skript *rollout.sh* vorkonfiguriert werden soll. Der Flash-Vorgang wird in diesen Fällen planmäßig fortgesetzt.

6.4 Das Gerät außer Betrieb nehmen (Decommissioning Mode)

ACHTUNG: Alle Daten auf dem Gerät werden unwiederruflich gelöscht. Das Gerät kann anschließend vom Kunden nicht wieder in Betrieb genommen werden.

ACHTUNG: Wenn Sie das Gerät außer Betrieb nehmen und gegen ein anderes mGuard-Gerät austauschen möchten, müssen Sie zunächst die Konfiguration des Gerätes als ATV-Datei oder auf einer SD-Karte sichern (siehe Anwenderhandbuch „Web-based Management“ UM DE FW MGUARD10 – 110191_de_xx).

Anwendungsfälle

- Das Gerät soll außer Betrieb genommen und entsorgt werden.
- Das Gerät soll außer Betrieb genommen und alle Daten auf dem Gerät sollen unwiderruflich gelöscht werden.
- Das Gerät soll außer Betrieb genommen und gegen ein anderes Gerät ausgetauscht werden.

Ergebnis

- Alle Daten auf dem Gerät werden unwiderruflich gelöscht oder überschrieben:
  - Dateisystem
  - Trusted Platform Module
  - eMMC-Speicher
  - Konfigurationen
  - Passwörter und private Schlüssel
  - Bootloader (wird mit der Werkseinstellung überschrieben)
- Das Gerät kann vom Kunden nicht wieder in Betrieb genommen werden.
- Das Gerät kann den Vorschriften entsprechend entsorgt werden.

6.4.1 Decommissioning (Durchführung)

FL MGUARD 2102/4302
FL MGUARD 2105/4305

Durchführung (Tragschienen-Geräte)

ACHTUNG: Alle Daten auf dem Gerät werden unwiederruflich gelöscht. Das Gerät kann vom Kunden nicht wieder in Betrieb genommen werden.

Sie können jeden einzelnen Schritt abbrechen, indem Sie die Spannungsversorgung unterbrechen oder 60 Sekunden warten, ohne eine Aktion durchzuführen.

- Drücken Sie die Mode-Taste 9-mal.
- Warten Sie ca. 2 Sekunden, bis die LEDs PF1 bis PF5 orange **leuchten.**
- Drücken Sie die Mode-Taste 9-mal.
- Warten Sie ca. 2 Sekunden, bis die LEDs PF1 bis PF5 orange **blinken.**
- Drücken Sie die Mode-Taste 3-mal.

↳ Alle Daten auf dem Gerät werden unwiderruflich gelöscht.
↳ Das Gerät wird automatisch neu gestartet.
↳ Der Vorgang ist abgeschlossen, wenn die LEDs PF1 bis PF5 rot blinken.
↳ Das Gerät kann vom Kunden nicht wieder in Betrieb genommen werden.

FL MGUARD 4102 PCI(E)

Durchführung (PCI-Karten)

ACHTUNG: Alle Daten auf dem Gerät werden unwiederruflich gelöscht. Das Gerät kann vom Kunden nicht wieder in Betrieb genommen werden.

Sie können jeden einzelnen Schritt abbrechen, indem Sie die Spannungsversorgung unterbrechen oder 60 Sekunden warten, ohne eine Aktion durchzuführen.

- Drücken Sie die Mode-Taste 9-mal.
- Warten Sie ca. 2 Sekunden, bis die **LED PF1** orange **leuchtet**.
- Drücken Sie die Mode-Taste 9-mal.
- Warten Sie ca. 2 Sekunden, bis die **LED PF1** orange **blinkt**.
- Drücken Sie die Mode-Taste 3-mal.

↳ Alle Daten auf dem Gerät werden unwiderruflich gelöscht.
↳ Das Gerät wird automatisch neu gestartet.
↳ Der Vorgang ist abgeschlossen, wenn die LED FAIL rot blinkt.
↳ Das Gerät kann vom Kunden nicht wieder in Betrieb genommen werden.

7 Gerätetausch, Gerätedefekt und Reparatur

7.1 Sicheres Löschen von sensitiven Daten / Außerbetriebnahme

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.

ACHTUNG: Alle Daten auf dem Gerät werden unwiederruflich gelöscht. Das Gerät kann anschließend vom Kunden nicht wieder in Betrieb genommen werden.

Gehen Sie wie folgt vor:

- Entnehmen Sie gegebenenfalls die SD-Karte.
- Führen Sie den Smart-Mode „Das Gerät außer Betrieb nehmen (Decommissioning Mode)“ aus, um alle Daten auf dem Gerät sicher zu löschen (siehe Kapitel 6.4).
- Verwahren Sie eine gegebenenfalls verwendete SD-Karte geschützt vor unbefugten Dritten auf oder löschen Sie deren Inhalt vollständig.

7.2 Gerätetausch

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

Gehen Sie bei einem Gerätetausch wie folgt vor:

- Sichern Sie die kundenspezifischen Daten (Konfigurationen, Passwörter, private Schlüssel, Zertifikate) auf einem externen Datenträger (SD-Karte/ECS).
- Entnehmen Sie die SD-Karte.
- Schalten Sie das Gerät spannungsfrei.
- Entfernen Sie alle Leitungen.
- Demontieren Sie das Gerät wie in Kapitel 3.3 und 4.3 beschrieben.
- Tauschen Sie das Gerät gegen ein identisches Gerät (gleiche Artikelnummer), fabrikneu oder mit Werkseinstellungen (siehe Kapitel 6), aus.
- Stellen Sie die gespeicherte Konfiguration des alten Gerätes auf dem neuen Gerät wieder her (siehe Kapitel 7.2.1).
- (Optional) Falls Sie das alte Geräte außer Betrieb nehmen möchten, führen Sie den Smart-Mode „Das Gerät außer Betrieb nehmen (Decommissioning Mode)“ aus. Alle Daten auf dem Gerät werden dabei sicher gelöscht (siehe Kapitel 6.4).

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

Mehr Informationen zur Verwendung von Konfigurationsprofilen finden Sie im Benutzerhandbuch UM DE FW MGUARD10 „Web-based Management“ im Phoenix Contact Web Shop unter phoenixcontact.net/product/1357828.

7.3 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 8).
  - 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.

7.4 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.

8 Technische Daten

8.1 FL MGUARD 4305/KX

Tabelle 8-1 Technische Daten (FL MGUARD 4305/KX)

Allgemeine Daten	
Plattform	Marvell Armada 3720
Netzwerk-Schnittstellen	5 Ethernet-Schnittstellen mit: – 3 LAN-Ports (managed switch) | 1 DMZ-Port | 1 WAN-Port – 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)	-40 °C … +60 °C
Umgebungstemperatur (Lagerung/Transport)	-40 °C … +70 °C
Zulässige Luftfeuchtigkeit (Betrieb)	5 % … 95 % (keine Betauung)
Schutzart	IP20 (not tested by UL)
Schutzklasse	Class III (VDE 0106; IEC 60536, nur für den Innenbereich)
Überspannungskategorie	Class II (IEC 61010-1)
Luftdruck (Betrieb)	68 kPa … 108 kPa, 3000 m ü.N.N.
Umgebungsverträglichkeit	Frei von lackbenetzungsstörenden Stoffen nach VW-Spezifikation
Verschmutzungsgrad	2
Einbaulage	Senkrecht auf einer Normtragschiene
Verbindung zur Funktionserde	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 Tragschiene)
Gewicht (exklusive Verpackung)	302 g
Gewicht (inklusive Verpackung)	446 g

Firmware- und Leistungswerte	
Unterstützte Firmware	ab mGuard 10.4.1
Management-Support	Web-based Management (HTTPS) | SSH | GAI Config | SD-Karte

Versorgungsspannung (US1/US2)	
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	12 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)	1,21 A
Typische Stromaufnahme (US= 24 V, T_{amb} = 25 °C, DO_I = 0/OFF)	0,16 A
Prüfspannung	500 V DC für eine Minute

Netzwerkschnittstellen	
Eigenschaften der RJ45-Anschlüsse	
Anzahl	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	12 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
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
Approbationen / Zulassungen	
ATEX	Ⓔx II 3 G Ex ec IIC T4 Gc (EN IEC 60079-0:2018, EN IEC 60079-7:2015/ A1:2018)
IECEx	Ex ec IIC T4 Gc (IEC 60079-0 Ed. 7 (2017-12) + Corr. 1 (2020-01), IEC 60079-7 Ed. 5.1 (2017-08))
UL, USA / Kanada	cULus
UL Ex, USA / Kanada	Class I, Division 2, Groups A, B, C und D, T4 Class I, Zone 2, AEx ec IIC T4 Ex ec IIC T4 Gc X UL 60079-0 Ed. 7 / UL 60079-7 Ed. 5, CSA C22.2 No. 60079-0 Ed. 4, CSA C22.2 No. 60079-7 Ed. 2
CCC / China-Ex	Ex ec IIC T4 Gc
UKCA Ex (UKEX)	Ⓔx II 3 G Ex ec IIC T4 Gc

8.2 FL MGUARD 4302/KX

Tabelle 8-2 Technische Daten (FL MGUARD 4302/KX)

Allgemeine Daten	
Plattform	Marvell Armada 3720
Netzwerk-Schnittstellen	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)
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)	-40 °C … +60 °C
Umgebungstemperatur (Lagerung/Transport)	-40 °C … +70 °C
Zulässige Luftfeuchtigkeit (Betrieb)	5 % … 95 % (keine Betauung)
Schutzart	IP20 (not tested by UL)
Schutzklasse	Class III (VDE 0106; IEC 60536, nur für den Innenbereich)
Überspannungskategorie	Class II (IEC 61010-1)
Luftdruck (Betrieb)	68 kPa … 108 kPa, 3000 m ü.N.N.
Umgebungsverträglichkeit	Frei von lackbenetzungsstörenden Stoffen nach VW-Spezifikation
Verschmutzungsgrad	2
Einbaulage	Senkrecht auf einer Normtragschiene
Verbindung zur Funktionserde	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 Tragschiene)
Gewicht (exklusive Verpackung)	302 g
Gewicht (inklusive Verpackung)	446 g

Firmware- und Leistungswerte	
Unterstützte Firmware	ab mGuard 10.4.1
Management-Support	Web-based Management (HTTPS) | SSH | GAI Config | SD-Karte

Versorgungsspannung (US1/US2)	
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	12 V DC … 36 V DC

Versorgungsspannung (US1/US2)	
Zulässige Welligkeit (innerhalb des zulässigen Spannungsbereichs)	3,6 V_{PP}
Maximal Stromaufnahme (US = Min, T_{amb} = Max, DO_I = Max)	1,12 A
Typische Stromaufnahme (US= 24 V, T_{amb} = 25 °C, DO_I = 0/OFF)	0,12 A
Prüfspannung	500 V DC für eine Minute

Netzwerkschnittstellen	
Eigenschaften der RJ45-Anschlüsse	
Anzahl	2
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	12 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
Approbationen / Zulassungen	
ATEX	Ⓔx II 3 G Ex ec IIC T4 Gc (EN IEC 60079-0:2018, EN IEC 60079-7:2015/ A1:2018)
IECEx	Ex ec IIC T4 Gc (IEC 60079-0 Ed. 7 (2017-12) + Corr. 1 (2020-01), IEC 60079-7 Ed. 5.1 (2017-08))
UL, USA / Kanada	cULus
UL Ex, USA / Kanada	Class I, Division 2, Groups A, B, C und D, T4 Class I, Zone 2, AEx ec IIC T4 Ex ec IIC T4 Gc X UL 60079-0 Ed. 7 / UL 60079-7 Ed. 5, CSA C22.2 No. 60079-0 Ed. 4, CSA C22.2 No. 60079-7 Ed. 2
CCC / China-Ex	Ex ec IIC T4 Gc
UKCA Ex (UKEX)	Ⓔx II 3 G Ex ec IIC T4 Gc

8.3 FL MGUARD 2105 / FL MGUARD 4305

Tabelle 8-3 Technische Daten (FL MGUARD 2105 / FL MGUARD 4305)

Allgemeine Daten	
Plattform	Marvell Armada 3720
Netzwerk-Schnittstellen	
FL MGUARD 2105	5 Ethernet-Schnittstellen mit: – 4 LAN-Ports (unmanaged switch) | 1 WAN-Port – 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 4305	5 Ethernet-Schnittstellen mit: – 3 LAN-Ports (managed switch) | 1 DMZ-Port | 1 WAN-Port – 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)	
FL MGUARD 2105	-20 °C … +60 °C
FL MGUARD 4305	-40 °C … +60 °C
Umgebungstemperatur (Lagerung/Transport)	-40 °C … +70 °C
Zulässige Luftfeuchtigkeit (Betrieb)	5 % … 95 % (keine Betauung)
Schutzart	IP20 (not tested by UL)
Schutzklasse	Class III (VDE 0106; IEC 60536, nur für den Innenbereich)
Überspannungskategorie	Class II (IEC 61010-1)
Luftdruck (Betrieb)	68 kPa … 108 kPa, 3000 m ü.N.N.
Umgebungsverträglichkeit	Frei von lackbenetzungsstörenden Stoffen nach VW-Spezifikation
Verschmutzungsgrad	2
Einbaulage	Senkrecht auf einer Normtragschiene
Verbindung zur Funktionserde	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 Tragschiene)
Gewicht (exklusive Verpackung)	302 g
Gewicht (inklusive Verpackung)	446 g

Firmware- und Leistungswerte	
Unterstützte Firmware	ab mGuard 10.2.0
Management-Support	Web-based Management (HTTPS) | SSH | GAI Config | SD-Karte

Versorgungsspannung (US1/US2) (US2 nur bei FL MGUARD 4305)	
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	12 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)	1,21 A
Typische Stromaufnahme (US= 24 V, T_{amb} = 25 °C, DO_I = 0/OFF)	0,16 A
Prüfspannung	500 V DC für eine Minute

Netzwerkschnittstellen	
Eigenschaften der RJ45-Anschlüsse	
Anzahl	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	12 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
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

8.4 FL MGUARD 2102 / FL MGUARD 4302

Tabelle 8-4 Technische Daten (FL MGUARD 2102 / FL MGUARD 4302)

Allgemeine Daten	
Plattform	Marvell Armada 3720
Netzwerk-Schnittstellen	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)
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)	
FL MGUARD 2102	-20 °C ... +60 °C
FL MGUARD 4302	-40 °C ... +60 °C
Umgebungstemperatur (Lagerung/Transport)	-40 °C ... +70 °C
Zulässige Luftfeuchtigkeit (Betrieb)	5 % ... 95 % (keine Betauung)
Schutzart	IP20 (not tested by UL)
Schutzklasse	Class III (VDE 0106; IEC 60536, nur für den Innenbereich)
Überspannungskategorie	Class II (IEC 61010-1)
Luftdruck (Betrieb)	68 kPa ... 108 kPa, 3000 m ü.N.N.
Umgebungsverträglichkeit	Frei von lackbenetzungsstörenden Stoffen nach VW-Spezifikation
Verschmutzungsgrad	2
Einbaulage	Senkrecht auf einer Normtragschiene
Verbindung zur Funktionserde	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 Tragschiene)
Gewicht (exklusive Verpackung)	302 g
Gewicht (inklusive Verpackung)	446 g

Firmware- und Leistungswerte	
Unterstützte Firmware	ab mGuard 10.0.0
Management-Support	Web-based Management (HTTPS) | SSH | GAI Config | SD-Karte

Versorgungsspannung (US1/US2) (US2 nur bei FL MGUARD 4302)	
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	12 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)	1,12 A
Typische Stromaufnahme (US= 24 V, T_{amb} = 25 °C, DO_I = 0/OFF)	0,12 A
Prüfspannung	500 V DC für eine Minute

Netzwerkschnittstellen	
Eigenschaften der RJ45-Anschlüsse	
Anzahl	2
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	12 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
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

8.5 FL MGUARD 4102 PCI / FL MGUARD 4102 PCIE

Tabelle 8-5 Technische Daten (FL MGUARD 4102 PCI(E)

Allgemeine Daten	
Plattform	Marvell Armada 3720
Netzwerk-Schnittstellen	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)
Stromversorgung	PCI: 3,3 V und 5 V PCIE: 3,3 V und 12 V Via PCI- oder PCI Express-Bus. Beachten Sie dabei die Hinweise in der Dokumentation zu Ihrem System.
Leistungsaufnahme	typisch T_{amb} = 25 °C Durchsatz 10 % (100 Mbit) = 2,72 W max. T_{amb} = 70 °C max. Durchsatz = 4,2 W
Maximal Stromaufnahme (US = Min, T_{amb} = Max)	
FL MGUARD 4102 PCI	3,3 V = 0,935 A 5 V = 0,33 A
FL MGUARD 4102 PCIE	3,3 V = 0,935 A 12 V = 0,1 A
Typische Stromaufnahme (T_{amb} = 25 °C, Auslastung 10 % Bandbreite)	
FL MGUARD 4102 PCI	3,3 V = 0,52 A 5 V = 0,24 A
FL MGUARD 4102 PCIE	3,3 V = 0,52 A 12 V = 0,093 A
Diagnose-Werkzeuge	Status- und Diagnose-LEDs | Log-Dateien
Besonderheiten	Echtzeituhr | Trusted Platform Module (TPM) | Temperatursensor
Umgebungstemperatur (Betrieb)	-40 °C ... +60 °C
Umgebungstemperatur (Lagerung/Transport)	-40 °C ... +70 °C
Zulässige Luftfeuchtigkeit (Betrieb)	5 % ... 95 % (keine Betauung)
Schutzart	je nach Einbauart, abhängig vom Wirtssystem
Schutzklasse	Class III (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

Allgemeine Daten	
Überspannungskategorie	Keine
Einbaulage	Freier PCI- oder PCI-Express-Steckplatz auf dem Wirtssystem
Verbindung zur Funktionserde	Über das Slotblech

Firmware	
Unterstützte Firmware	ab mGuard 10.1.0
Management-Support	Web-based Management (HTTPS) | SSH | GAI Config | SD-Karte

Netzwerkschnittstellen	
Eigenschaften der RJ45-Anschlüsse	
Anzahl	2
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)

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
Störfestigkeit nach EN 61000-4-2 (IEC 1000-4-2) (ESD) Kontaktentladung: Luftentladung: indirekte Entladung:	Anforderungen gem. DIN EN 61000-6-2 Prüfschärfegrad 3, Beurteilungskriterium B Prüfschärfegrad 3, Beurteilungskriterium B 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

Konformität zu EMV-Richtlinien	
Störfestigkeit nach EN 61000-4-4 (IEC1000-4-4) (Burst) Datenleitungen:	Anforderungen gem. DIN EN 61000-6-2 Prüfschärfegrad 3, Beurteilungskriterium A
Störfestigkeit nach EN 61000-4-5 (IEC1000-4-5) (Surge) Datenleitungen:	Anforderungen gem. DIN EN 61000-6-2 Prüfschärfegrad 2, Beurteilungskriterium B

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
Email: info@phoenixcontact.com
phoenixcontact.com

110192_de_08
Item No. –08