



Smart Ethernet Box

Anwenderhandbuch

Anwenderhandbuch

Smart Ethernet Box

UM DE SCX xPOE..., Revision 04

2025-05-21

Dieses Handbuch ist gültig für:

Bezeichnung	Hardware-Version	Software-Release	Artikel-Nr.
SCX 4POE 2LX	21	1.11	1102626
SCX 2POE 2LX	21	1.11	1108543
SCX 4POE 2T	21	1.11	1108542
SCX 2POE 2T	21	1.11	1108544

Inhaltsverzeichnis

1	Zu Ihrer Sicherheit	5
1.1	Kennzeichnung der Warnhinweise	5
1.2	Qualifikation der Benutzer	5
1.3	Einsatzbereich des Produkts.....	6
1.4	Sicherheitshinweise	7
1.5	Elektrischer Anschluss.....	7
1.6	UL-Hinweise	8
1.7	Sicherheit im Netzwerk	10
1.8	Anwenderdokumentation	11
2	Transportieren, Lagern und Auspacken	12
2.1	Transportieren.....	12
2.2	Lagern	12
2.3	Auspacken	13
3	Produktbeschreibung	14
3.1	Lizenzhinweise zu Open Source Software	15
3.2	Aufbau.....	16
4	Installieren	22
4.1	Montieren und demontieren	22
4.2	Elektrischer Anschluss.....	30
4.3	Inbetriebnahme.....	39
5	Konfigurieren	41
5.1	Web-based Management.....	41
5.2	Mode-Taster	73
5.3	Verhalten bei Neustart und im Fehlerfall	75
6	Gerätetausch, Gerätedefekt und Reparatur	76
6.1	Gerätetausch	76
6.2	Gerätedefekt und Reparatur	78
7	Wartung und Entsorgung	79
7.1	Wartung	79
7.2	Entsorgung.....	80

8	Technische Daten	81
8.1	Bestelldaten	81
8.2	Technische Daten	83
8.3	Abmessungen	89
8.4	Prinzipschaltbild	91
A	Technischer Anhang	92
A 1	Frame-Switching	92
A 2	RSTP - Rapid Spanning Tree Protocol	94
A 3	SNMP - Simple Network Management Protocol	102
A 4	LLDP - Link Layer Discovery Protocol	104
B	Verzeichnisanhang	107
B 1	Abbildungsverzeichnis	107
B 2	Tabellenverzeichnis	109
B 3	Stichwortverzeichnis	111
C	Änderungsnachweis	114

1 Zu Ihrer Sicherheit



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

1.1 Kennzeichnung der Warnhinweise



Dieses Symbol kennzeichnet Gefahren, die zu Personenschäden führen können.

Es gibt drei Signalwörter für die Schwere der möglichen Verletzung.

GEFAHR

Hinweis auf eine Gefährdung mit hohem Risikograd. Wenn die Gefährdung nicht vermieden wird, hat sie den Tod oder eine schwere Verletzung zur Folge.

WARNUNG

Hinweis auf eine Gefährdung mit mittlerem Risikograd. Wenn die Gefährdung nicht vermieden wird, kann sie den Tod oder eine schwere Verletzung zur Folge haben.

VORSICHT

Hinweis auf Gefährdung mit niedrigem Risikograd. Wenn die Gefährdung nicht vermieden wird, kann sie eine geringfügige oder mäßige Verletzung zur Folge haben.



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.



Dieses Symbol weist auf ein Risiko für Security-Probleme in der industriellen Automatisierung hin. Hier finden Sie Informationen darüber, wie Sie Security-Problemen vorbeugen können.

1.2 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.
- Die Anwender müssen mit dem Einsatz von Ethernet-Netzwerkkomponenten vertraut sein.

Beim Einsatz von Ethernet-Netzwerkkomponenten besteht die Gefahr von Datenkonflikten durch Fehlbedienung sowie eine Gefährdung der Daten- und Netzwerkintegrität durch unbefugten Datenzugriff. Um den Einsatz der Geräte und die vorgenommene Konfiguration zu beurteilen, ziehen Sie im Zweifel einen Ethernet-Netzwerkspezialisten hinzu.

1.3 Einsatzbereich des Produkts

1.3.1 Bestimmungsgemäße Verwendung

Die Smart Ethernet Box dient zum Verbinden von PoE-Endgeräten, z. B. von IP-Kameras mit einem Video-Server. Über die Smart Ethernet Box können Sie PoE-Endgeräte und weitere externe Geräte mit Spannung versorgen.

Die Smart Ethernet Box ist für die feste Montage im Innen- oder Außenbereich ausgelegt.



Das zugelassene Zubehör finden Sie am Produkt unter phoenixcontact.com/products.

1.3.2 Veränderungen des Produkts

- Veränderungen, An- oder Umbauten an der Smart Ethernet Box sind **nicht** zulässig.
- Öffnen oder Verändern der enthaltenen Komponenten sind **nicht** zulässig.
- Modifikationen an der Hard- und Firmware sind **nicht** zulässig.
- Sie können Geräte auf der integrierten Tragschiene der Smart Ethernet Box installieren. Beachten Sie unbedingt die Anweisungen im Kapitel „Zusätzliche Geräte installieren“ auf Seite 38.

Unsachgemäße Arbeiten oder Veränderungen können Ihre Sicherheit gefährden oder die Smart Ethernet Box beschädigen. Sie dürfen die Smart Ethernet Box oder die enthaltenen Komponenten nicht reparieren.

- Wenn die Smart Ethernet Box einen Defekt hat, wenden Sie sich an Phoenix Contact.

Erweiterbare Kabelverschraubung

Es ist zulässig, eine der Kabelverschraubungen für die Versorgungsleitung auf M32 zu vergrößern. Dies erfolgt auf Verantwortung des Kunden.

- Die zugesicherten Eigenschaften des Geräts, insbesondere zu Dichtigkeit und Schutzart, sind nicht mehr sichergestellt.
- Die Dichtigkeit des Gehäuses muss kundenseitig sichergestellt werden. Beachten Sie die Anwenderdokumentation des Herstellers der Kabelverschraubung.
- Die UL-Zulassung erlischt.
- Beachten Sie die Anweisungen unter „Erweiterbare Kabelverschraubung für Versorgungsleitung“.

1.4 Sicherheitshinweise



Die Installation, Bedienung und Wartung ist von elektrotechnisch qualifiziertem Fachpersonal durchzuführen. Befolgen Sie die beschriebenen Installationsanweisungen.

- 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.
- Der einwandfreie und sichere Betrieb der Smart Ethernet Box ist nur bei sachgemäßem Transport, sachgemäßer Lagerung, Aufstellung, Montage, Installation, Inbetriebnahme, Bedienung und Instandhaltung sichergestellt. Halten Sie die zulässigen Umgebungsbedingungen ein.

1.5 Elektrischer Anschluss



WARNUNG: Lebensgefahr durch Stromschlag!

Beim Betrieb können bestimmte Teile der Smart Ethernet Box unter gefährlicher Spannung stehen.

- Sehen Sie in der Nähe der Smart Ethernet Box einen Schalter/Leistungsschalter vor, der als Trennvorrichtung für dieses Gerät gekennzeichnet ist.
- Sehen Sie eine Überstromschutzeinrichtung ($I = 6 \dots 16 \text{ A}$) in der Installation vor.
- Verwenden Sie nur Leitungen, die den vorgeschriebenen Installationsvorschriften hinsichtlich Spannung, Strom, Isolationsmaterial, Belastbarkeit etc. entsprechen.
- Trennen Sie die Smart Ethernet Box bei Wartungsarbeiten von allen Energiequellen. Der Schalter in der Smart Ethernet Box schaltet diese **nicht** spannungsfrei!
- Verbinden oder trennen Sie die Anschlussleitungen niemals unter Last.

Gehen Sie bei Inbetriebnahme- und Wartungsarbeiten nach den fünf Sicherheitsregeln der EN 50110-1 vor:

1. Freischalten
2. Gegen Wiedereinschalten sichern
3. Spannungsfreiheit feststellen
4. Erden und Kurzschließen
5. Benachbarte, unter Spannung stehende Teile abdecken oder abschränken

Nach Abschluss der Arbeiten heben Sie die getroffenen Maßnahmen in der umgekehrten Reihenfolge wieder auf.

1.6 UL-Hinweise

Um das Gerät entsprechend der UL/CSA/IEC Standards zu installieren, müssen die folgenden Hinweise beachtet werden.



VORSICHT:

- Die äußeren Schaltkreise, die an dieses Gerät angeschlossen werden sollen, mit Ausnahme der Netzversorgung des Betriebsmittels, müssen durch verstärkte oder doppelte Isolierung galvanisch vom Netz oder gefährlichen Spannungen getrennt sein und die Anforderungen der NEC Class 2 oder SELV/PELV - Limited Energy der UL/CSA 61010-1, -2-201 oder Limited Power Source der UL/CSA 60950 erfüllen.
- Kommunikationskabel müssen die Anforderungen der Normen UL Standard 444 / CSA Standard (C22.2) Nr. 214 erfüllen, für den Einsatz geeignet und mit „Outdoor“ gekennzeichnet sein, um auf die Eignung für die Verlegung im Außenbereich von Wohnhäusern hinzuweisen.
- SFP-Transceiver müssen die entsprechenden Anforderungen der Normen UL 60950-1, CAN/CSA C22.2 Nr. 60950-1 erfüllen, als „Laserklasse I“ eingestuft sein und mit 21 CFR 1040 - Laser Class übereinstimmen.
- Das Gerät ist wartungsfrei konzipiert. Es ist nicht erlaubt, Reparaturen vorzunehmen.
- Das Anschlussstück (Kabelführungsadapter) muss mit der Kabelführung verbunden werden, bevor es mit dem Gehäuse verbunden wird.



Information:

- Der Schalter oder Leistungsschalter muss Teil der Installation sein, angemessen positioniert, leicht erreichbar und als Abtrennvorrichtung für das Betriebsmittel gekennzeichnet sein. Gibt es nur ein Gerät – einen Schalter oder einen Leistungsschalter – sind die Symbole 9 und 10 aus der Tabelle 1 der Norm UL/CSA/IEC 61010 ausreichend, wenn die Symbole auf oder neben dem Schalter bzw. Leistungsschalter aufgedruckt sind.
 - a) Leistungsschalter, die als Trennvorrichtung eingesetzt werden, müssen die entsprechenden Anforderungen der Normen UL Standard 489 / CSA Standard (C22.2) Nr. 5 / IEC 60947-2 erfüllen, für den Einsatz geeignet und in der Nähe des Betriebsmittels angebracht sein.
 - b) Schalter, die als Abtrennvorrichtung genutzt werden, müssen die entsprechenden Anforderungen der Normen UL Standard 508 / CSA Standard (C22.2) Nr. 14 / IEC 60947-3 erfüllen, für den Einsatz geeignet und in der Nähe des Betriebsmittels angebracht sein.
- Betriebsmittel, die aus dem Netz gespeist werden sollen, müssen durch Schmelzsicherungen, Leistungsschalter, Thermosicherungen, Impedanz-Begrenzungsschaltungen oder ähnliche Mittel gesichert sein, um sie vor übermäßiger Stromaufnahme aus dem Netz im Falle eines Fehlers im Betriebsmittel zu schützen.
 - a) Überstromschutzgeräte dürfen nicht in den Schutzleiter eingefügt werden. Sicherungen oder einpolige Leistungsschalter dürfen nicht in den Neutralleiter mehrphasiger Betriebsmittel eingefügt werden.
 - b) Ein einpoliger Leistungsschalter, der als Überstromschutz genutzt wird, muss in den ungeerdeten Versorgungsleiter geschaltet werden.
 - c) Ein mehrpoliger Leistungsschalter, der als Überstromschutz genutzt wird, muss so aufgebaut sein, dass er alle neutralen (geerdeten) und ungeerdeten Leiter der Netzversorgung gleichzeitig unterbricht.

- d) Sicherungen müssen die entsprechenden Anforderungen der Normen UL Standard 248 / CSA-Norm (C22.2) Nr. 248 / IEC 60127 erfüllen, für den Einsatz geeignet und in der Nähe des Betriebsmittels angebracht sein.
- e) Eine einzelne Sicherung, die als Überstromschutz genutzt wird, muss in den ungeerdeten Versorgungsleiter geschaltet werden.
- f) Wenn Sicherungen sowohl im neutralen (geerdeten) als auch im ungeerdeten Versorgungsleiter als Überstromschutz genutzt werden, müssen die Sicherungshalter nebeneinander montiert werden und die Sicherungen die gleiche KLASSIFIZIERUNG haben und dieselben Eigenschaften aufweisen.
- g) Die Schraubhülse eines Stecksicherungshalters und der ZUGÄNGLICHE Kontakt eines Abziehsicherungshalters, der mit dem ungeerdeten Versorgungsleiter verbunden ist, sind zur Last hin anzuschließen. Der ZUGÄNGLICHE Kontakt oder die Schraubhülse von Sicherungshaltern, die im neutralen (geerdeten) Leiter angeschlossen sind, müssen sich zur geerdeten Versorgungsleitung hin befinden.
- Die Schutzfunktion des Betriebsmittels kann eingeschränkt sein, wenn es nicht bestimmungsgemäß verwendet wird.
- Mindesttemperaturwert des Kabels, das an die Feldverdrahtungsklemmen angeschlossen werden soll (Netzversorgung)
75 °C, AWG 24 ... 10
Verwenden Sie ausschließlich Kupferleiter.
- Mindesttemperaturwert des Kabels, das an die Feldverdrahtungsklemmen angeschlossen werden soll (digitaler Ausgang)
75 °C, AWG 24 ... 16
Verwenden Sie ausschließlich Kupferleiter.

1.7 Sicherheit im Netzwerk



ACHTUNG: Netzwerksicherheit durch unbefugte Zugriffe gefährdet

Wenn Geräte mit einem Netzwerk verbunden sind, besteht die Gefahr von unbefugten Netzwerkzugriffen.

Beachten Sie die folgenden Sicherheitshinweise:

- Falls möglich, deaktivieren Sie nicht verwendete Kommunikationskanäle.
- Verwenden Sie sichere Passwörter, deren Komplexität und Lebensdauer dem Stand der Technik entsprechen.
- Beschränken Sie den Gerätezugriff auf autorisierte Personen. Begrenzen Sie die Anzahl der autorisierten Personen auf das notwendige Minimum.
- Installieren Sie immer die neueste Firmware-Version. Die Firmware steht am Artikel zum Download bereit (phoenixcontact.com/products).
- Beachten Sie die IT-Sicherheitsanforderungen und die geltenden Normen für Ihren Einsatzbereich. Treffen Sie die notwendigen Schutzmaßnahmen. Das können z. B. virtuelle Netzwerke für Fernwartungszugriffe oder eine Firewall sein.
- Setzen Sie das Gerät in sicherheitskritischen Anwendungen nur mit einer zusätzlichen Security-Appliance ein.
- Phoenix Contact bietet als Security-Appliance die Produktlinie mGuard an. Die mGuard-Router verbinden verschiedene Netzwerke zur Fernwartung und Absicherung des lokalen Netzwerks und schützen sie vor Cyber-Angriffen.
- Berücksichtigen Sie bei der Netzwerkplanung grundsätzlich Defense-in-Depth-Mechanismen.



Weitere Schutzmaßnahmen gegen unbefugte Netzwerkzugriffe finden Sie im Anwenderhinweis „INDUSTRIAL SECURITY“. Der Anwenderhinweis steht am Artikel zum Download bereit (phoenixcontact.com/products).

Deutsch: AH DE INDUSTRIAL SECURITY, 107913

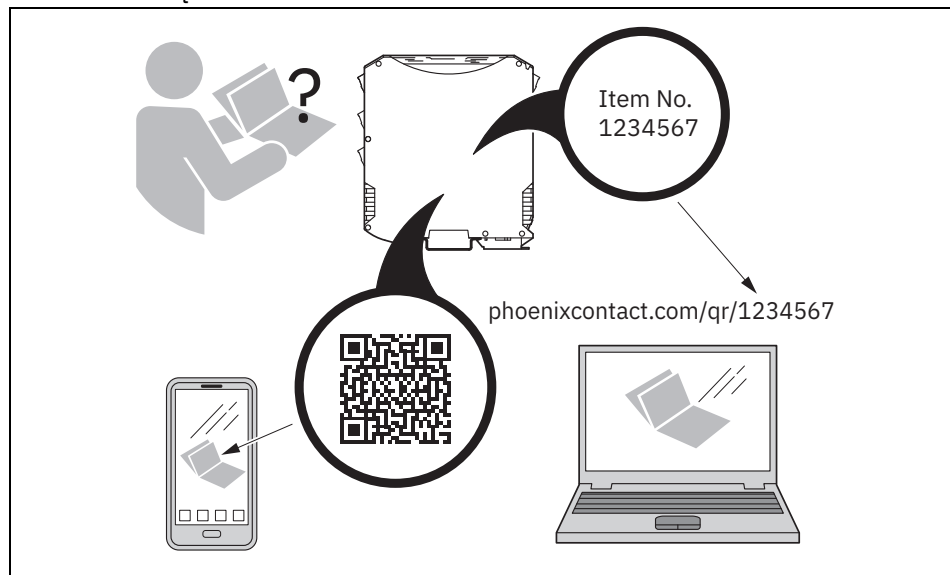
Englisch: AH EN INDUSTRIAL SECURITY, 107913

Wenn eine Sicherheitslücke bei Produkten, Lösungen und Dienstleistungen von Phoenix Contact vorliegt, wird diese auf der Webseite des PSIRT (Product Security Incident Response Team) veröffentlicht: phoenixcontact.com/psirt

1.8 Anwenderdokumentation

- Lesen Sie vor der Installation und Inbetriebnahme die Anwenderdokumentation.
- Die vollständige Anwenderdokumentation finden Sie im Internet unter „phoenixcontact.com/qr/xxx“. Ersetzen Sie „xxx“ durch die Artikelnummer des Produkts.
- Sie können auch den QR-Code auf dem Produkt benutzen. Sie finden den QR-Code hier:
 - Bis Hardware-Version 20: auf der Spleißkassette rechts neben dem Spleißbereich
 - Ab Hardware-Version 21: oben links neben den LEDs

Bild 1-1 QR-Code scannen



2 Transportieren, Lagern und Auspacken

2.1 Transportieren

Die Smart Ethernet Box wird in Kartonage verpackt geliefert.

- Transportieren Sie die Smart Ethernet Box nur originalverpackt an den Bestimmungsort.
- Beachten Sie die Hinweise zur Handhabung auf der Verpackung.
- Beachten Sie beim Transport die Angaben zur Luftfeuchtigkeit und zum Temperaturbereich (siehe hierzu „[Umgebungsbedingungen](#)“ auf Seite 87).
- Verwenden Sie zum Entladen und für den Transport ausschließlich geeignete und zugelassene Hebe- und Transportwerkzeuge.
- Sichern Sie die Smart Ethernet Box während des Transports. Beachten Sie dabei den Schwerpunkt. Gleiches gilt bei Umzügen, Umlagerung oder Rücksendungen. Der innerbetriebliche Transport ist nur gestattet, wenn das Transportgut ausreichend gegen Verrutschen und Herabfallen gesichert ist.
- Steigen Sie nicht auf die Smart Ethernet Box oder die Verpackung.
- Falls erforderlich, schützen Sie die Oberflächen vor Beschädigung.
- Achten Sie beim Transportieren oder Zwischenlagern darauf, dass die Oberflächen witterungsgeschützt, trocken, sauber und vor Fremdeinwirkung geschützt sind.

2.2 Lagern

Der Lagerort muss folgende Bedingungen erfüllen:

- Trocken
 - Geschützt vor Fremdeinwirkung
 - Geschützt vor schädlichen Umwelteinflüssen wie z. B. UV-Licht
-
- Beachten Sie für die Lagerung die Angaben zum Temperaturbereich sowie zur Luftfeuchtigkeit und Luftdruck.
Siehe „[Umgebungsbedingungen](#)“ auf Seite 87.

2.3 Auspacken

Lieferumfang

- Smart Ethernet Box
- Montageadapter
- 3x Blindstopfen M20
- 5x Blindstopfen M25

Bei den Varianten SCX ...POE 2LX zusätzlich:

- Spleißkamm
- 10x Kabelbinder



ACHTUNG: Elektrostatische Entladung

Elektrostatische Entladung kann Bauelemente beschädigen oder zerstören

- Beachten Sie beim Umgang die notwendigen Sicherheitsmaßnahmen gegen elektrostatische Entladung (ESD) nach EN 61340-5-1 und IEC 61340-5-1.

Lieferung kontrollieren

- Prüfen Sie die Smart Ethernet Box sowie die darin enthaltenen Komponenten auf Beschädigungen. Die Inbetriebnahme der Smart Ethernet Box mit beschädigtem Gehäuse oder beschädigten Komponenten ist nicht zulässig

Jede Beschädigung der Verpackung ist ein Hinweis auf einen möglichen transportbedingten Schaden. Ein Funktionsausfall kann möglich sein.

- Prüfen Sie den Verpackungsinhalt unmittelbar nach Anlieferung anhand des Lieferscheins auf Vollständigkeit.
- Reklamieren Sie entstandene Transportschäden sofort und informieren Sie umgehend Phoenix Contact oder Ihren Lieferanten sowie das Transportunternehmen.
- Fügen Sie Ihrer Reklamation aussagekräftige Fotos der beschädigten Verpackung/der beschädigten Lieferung bei.
- Bewahren Sie Versandkartons und Verpackungsmaterial zwecks möglicher Rücksendung auf.
- Verwenden Sie bei Rücksendung vorzugsweise die Originalverpackung.
- Beachten Sie die folgenden Hinweise, falls die Originalverpackung nicht mehr vorliegt:
 - Beachten Sie beim Transport die Angaben zur Luftfeuchtigkeit und zum Temperaturbereich (siehe hierzu „[Umgebungsbedingungen](#)“ auf Seite 87).
 - 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.

3 Produktbeschreibung



Die Smart Ethernet Box dient als Industrial-Outdoor-Switch zum Verbinden von PoE-Endgeräten, z. B. von IP-Kameras mit einem Video-Server. Über die Smart Ethernet Box können Sie PoE-Endgeräte und weitere externe Geräte mit Spannung versorgen.

Die Box integriert die Funktionalitäten herkömmlicher, mit Standard-Tragschienenengeräten bestückter Anschlusskästen in einem kompakten Gerät. So sparen Sie Planung und Installation.

Zahlreiche Management- und Monitoring-Funktionen stellen den zuverlässigen Betrieb der Anlage sicher.

Merkmale

- Kostenersparnis durch eine All-in-One-Lösung, die sämtliche Funktionalitäten in einem Gerät bereitstellt
- Managed Ethernet Switch mit RSTP, VLAN, SNMP und weiteren Funktionen
- Bis zu 40 Geräte im Ring mit RSTP, bis zu 70 Geräte im Ring mit LTS
- Hohe Zeitersparnis durch Adapter zur Wand- und Mastmontage
- Minimaler Verdrahtungsaufwand
- Austauschbarer Überspannungsschutz
- Zahlreiche Alarmmeldungen per SNMP wie z. B. bei Sabotageversuchen oder defektem Überspannungsschutz
- Überwachung der Tür über SNMP, automatische Benachrichtigung bei unerlaubtem Öffnen
- Weitbereichsnetzteil 100 ... 240 V AC
- Erweitertes PoE-Management für den zuverlässigen Betrieb von IP-Kameras und anderen PoE-Endgeräten
- Einfache und schnelle Inbetriebnahme und Konfiguration über das Web-based Management oder die Software FL Network Manager
- Zusätzliche Tragschiene für optionale Geräte wie z. B. Überspannungsschutz für die Uplink-Ports, WLAN Access Point, Mobilfunk-Router etc.
- Wasserdichtes und schlagfestes Gehäuse aus Polycarbonat
- Bei den Produktvarianten ...2LX: Integrierte Spleißkassette für die sichere Ablage von Faserverbindungen und Faserreserven

Tabelle 3-1 Übersicht Produktvarianten

Bezeichnung	Anzahl PoE-Ports	Uplink-Ports
SCX 4POE 2LX	4	2 SFP-Slots
SCX 2POE 2LX	2	SFP-Module als Zubehör erhältlich, siehe „Zubehör“
SCX 4POE 2T	4	2 RJ45-Buchsen
SCX 2POE 2T	2	

3.1 Lizenzhinweise zu Open Source Software

Die Lizenzhinweise finden Sie im Web-based Management des Geräts.

- Klicken Sie in der Fußzeile des Web-based Managements auf „Licenses and Legal Information“.

3.1.1 Hinweise zu LGPL-Software-Bibliotheken

Jede Open Source Software, die im Produkt verwendet wird, unterliegt den jeweiligen Lizenzbestimmungen, die von den Phoenix Contact-Software-Lizenzbedingungen (Software License Terms (SLT)) für das Produkt nicht berührt werden.

Insbesondere kann der Lizenznehmer die jeweilige Open Source Software entsprechend den geltenden Lizenzbestimmungen ändern. Falls der Lizenznehmer eine in diesem Produkt enthaltene LGPL-Software-Bibliothek ändern möchte, ist Reverse Engineering für das Debuggen solcher Modifikationen zulässig.

3.1.2 Hinweise zu OpenSSL

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)

3.1.3 Quellcode anfordern

Die Geräte beinhalten Software-Komponenten, die vom Rechteinhaber als freie Software oder Open Source Software unter der GNU General Public License lizenziert sind.

Sie können den Quellcode dieser Software-Komponenten gegen eine Bearbeitungsgebühr von 50 Euro innerhalb von drei Jahren nach Auslieferung des Geräts in Form einer CD oder DVD-ROM anfordern.

Kontaktieren Sie hierzu schriftlich den After-Sales-Service von Phoenix Contact unter der Adresse

PHOENIX CONTACT GmbH & Co. KG
After Sales Service
Flachsmarkstraße 8
32825 Blomberg
GERMANY

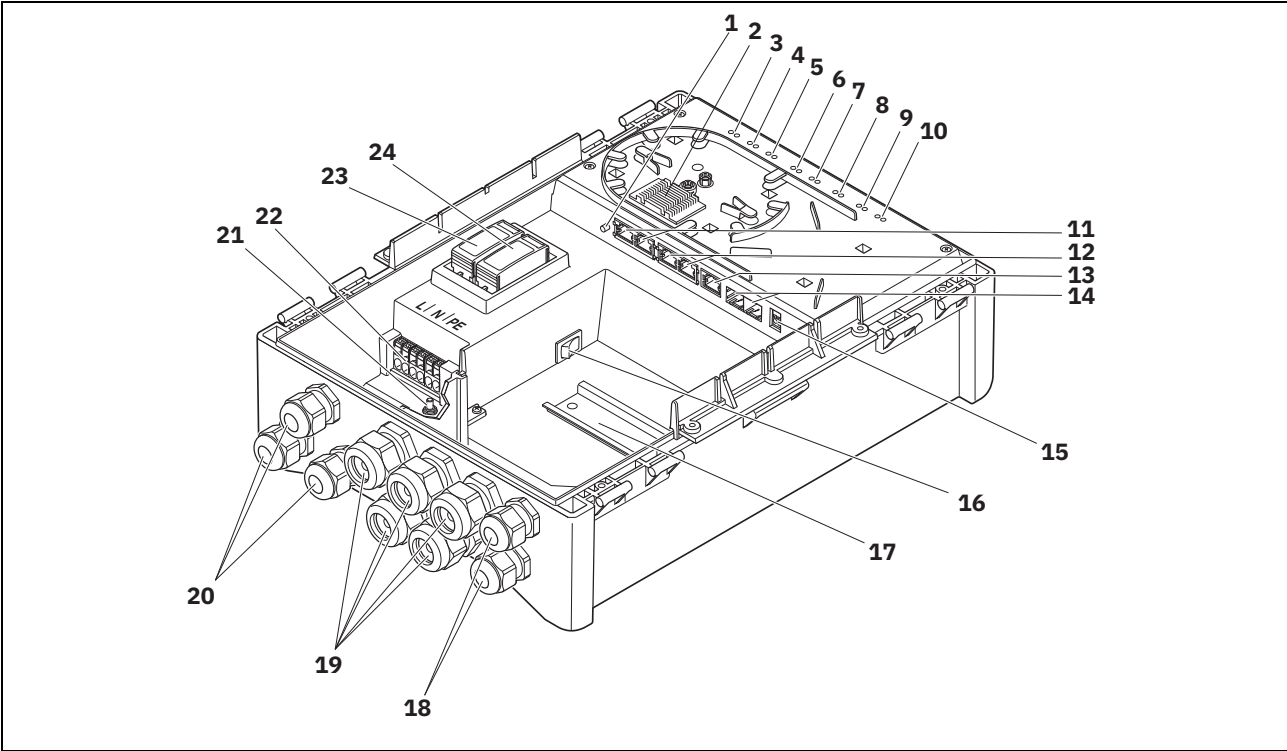
Betreff:

Source Code Smart Ethernet Box

3.2 Aufbau

3.2.1 SCX xPOE 2LX

Bild 3-1 Smart Ethernet Box mit LWL-Anschlüssen



1	MODE	Mode-Taster
2	Spleißkamm	
3... 10	LEDs	siehe Tabelle 3-2
11	POE3/4	Power-over-Ethernet-Ports 3 und 4 (nur SCX 4POE 2LX)
12	POE1/2	Power-over-Ethernet-Ports 1 und 2
13	CONF	Lokaler Konfigurations-Port
14	UP1/2	SFP-Slots (SFP-Module als Zubehör erhältlich)
15	+/- AUX	24 V DC, Schaltausgang, Konfiguration über Web-based Management
16	Schalter, Gerät Ein/Aus	

17	Tragschiene zum Installieren zusätzlicher Geräte
18	Kabelverschraubung M20 (Daten, Kleinspannungszone, <50 V AC / < 120 V DC)
19	Kabelverschraubung M25 (Daten, Kleinspannungszone, <50 V AC / < 120 V DC)
20	Kabelverschraubung M20 (Versorgung, Netzspannungszone)
21	Erdungsschraube
22	Push-in-Anschluss, Versorgungsspannung, 100 ... 240 V AC
23	Überspannungsschutz, steckbar
24	Überspannungsschutz, steckbar

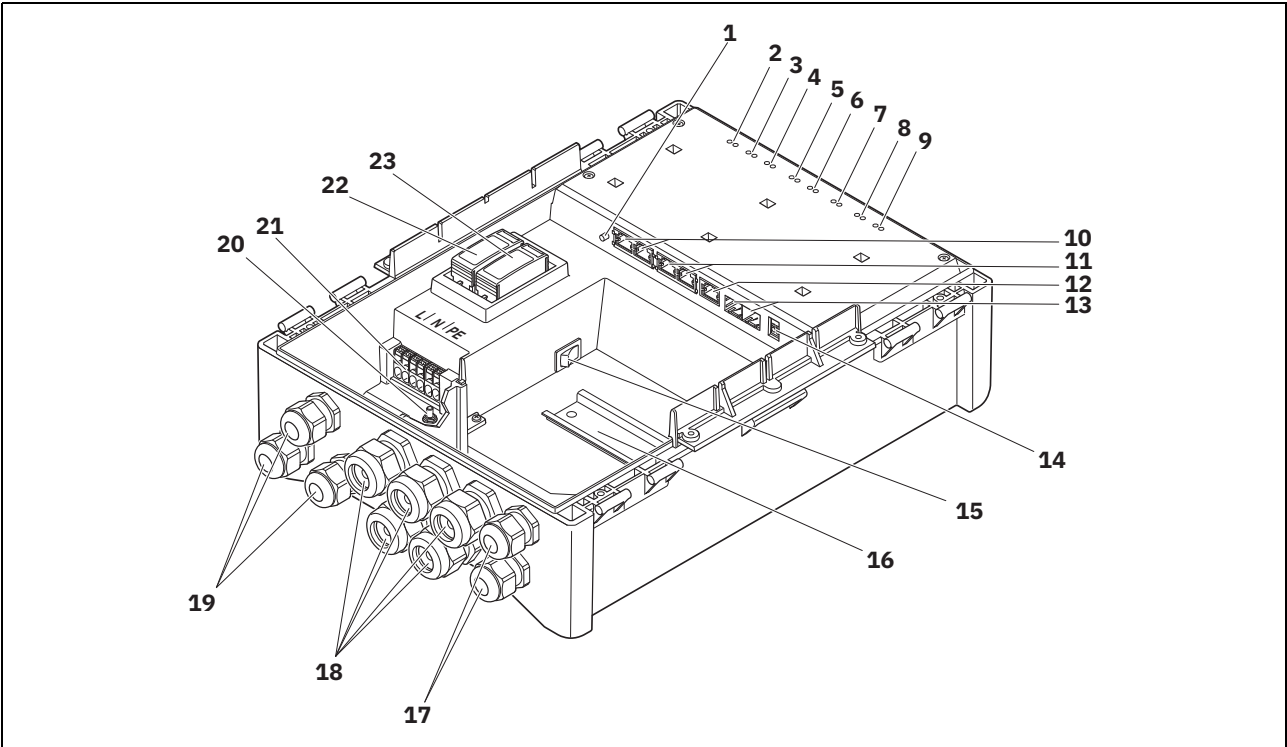
Tabelle 3-2 LEDs SCX xPOE 2LX

Pos.	LED	Status		Bedeutung
3	PWR	Grün	Ein	Gerät eingeschaltet
	AUX	Grün	Ein	24 V DC am Schaltausgang +/- AUX
4... 10	LINK...	-	Aus	Kein Ethernet-Link
		Grün	Ein	10/100 MBit/s, Verbindung aufgebaut
			Flackernd	10/100 MBit/s, Daten werden übertragen
		Orange	Ein	1000 MBit/s, Verbindung aufgebaut
			Flackernd	1000 MBit/s, Daten werden übertragen
		4...7	POE...	-
Grün	Blinkt			Automodus, Suche nach Powered Device (PD)
	Ein			Automodus, PD wird über PoE versorgt.
Orange	Ein			Force-Modus ¹ , PoE-Spannung liegt am Port an
	Blinkt			Fehler, z. B. ausgehandelte Leistung überschritten, PD wird nicht versorgt
Alle LEDs				Grün

¹ Im Force-Modus können Sie anhand der LEDs **nicht** unterscheiden, ob ein PD mit Leistung versorgt wird.

3.2.2 SCX xPOE 2T

Bild 3-2 Smart Ethernet Box mit RJ45-Anschlüssen



1	MODE	Mode-Taster
2... 9	LEDs	siehe Tabelle 3-3
10	POE3/4	Power-over-Ethernet-Ports 3 und 4 (nur SCX 4POE 2T)
11	POE1/2	Power-over-Ethernet-Ports 1 und 2
12	CONF	Lokaler Konfigurations-Port
13	UP1/2	Ethernet-Uplink-Ports
14	+/- AUX	24 V DC, Schaltausgang, Konfiguration über Web-based Management
15	Schalter, Gerät Ein/Aus	

16	Tragschiene zum Installieren zusätzlicher Geräte
17	Kabelverschraubung M20 (Daten, Kleinspannungs- zone, <50 V AC / < 120 V DC)
18	Kabelverschraubung M25 (Daten, Kleinspannungs- zone, <50 V AC / < 120 V DC)
19	Kabelverschraubung M20 (Versorgung, Netzspan- nungszone)
20	Erdungsschraube
21	Push-in-Anschluss, Versorgungsspannung, 100 ... 240 V AC
22	Überspannungsschutz, steckbar
23	Überspannungsschutz, steckbar

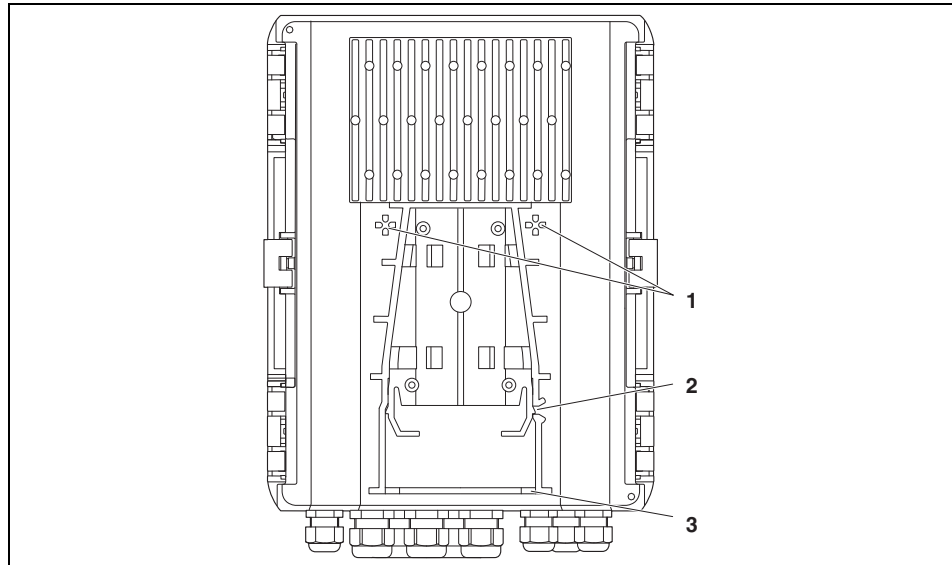
Tabelle 3-3 LEDs SCX xPOE 2T

Pos.	LED	Status		Bedeutung
2	PWR	Grün	Ein	Gerät eingeschaltet
	AUX	Grün	Ein	24 V DC am Schaltausgang +/- AUX
3...9	LINK...	-	Aus	Kein Ethernet-Link
		Grün	Ein	10/100 MBit/s, Verbindung aufgebaut
			Flackernd	10/100 MBit/s, Daten werden übertragen
		Orange	Ein	1000 MBit/s, Verbindung aufgebaut
			Flackernd	1000 MBit/s, Daten werden übertragen
		3...6	POE...	-
Grün	Blinkt			Automodus, Suche nach Powered Device (PD)
	Ein			Automodus, PD wird über PoE versorgt.
Orange	Ein			Force-Modus ¹ , PoE-Spannung liegt am Port an
	Blinkt			Fehler, z. B. ausgehandelte Leistung überschritten, PD wird nicht versorgt
Alle LEDs				Grün

¹ Im Force-Modus können Sie anhand der LEDs nicht unterscheiden, ob ein PD mit Leistung versorgt wird oder nicht.

3.2.3 Rückseite

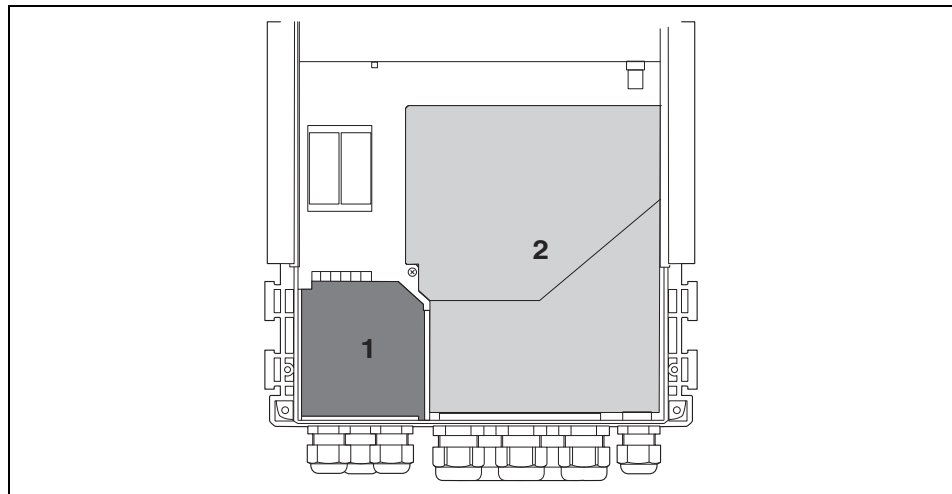
Bild 3-3 Rückseite



- 1 Öffnungen mit Klimamembran gegen Kondensatbildung
- 2 Demontageöffnung, seitlich
- 3 Demontageöffnung, unten

3.2.4 Zonen in der Smart Ethernet Box

Bild 3-4 Zonen in der Smart Ethernet Box



- 1 Netzspannungszone
- 2 Kleinspannungszone (<50 V AC / <120 V DC)

3.2.5 Gehäuse öffnen

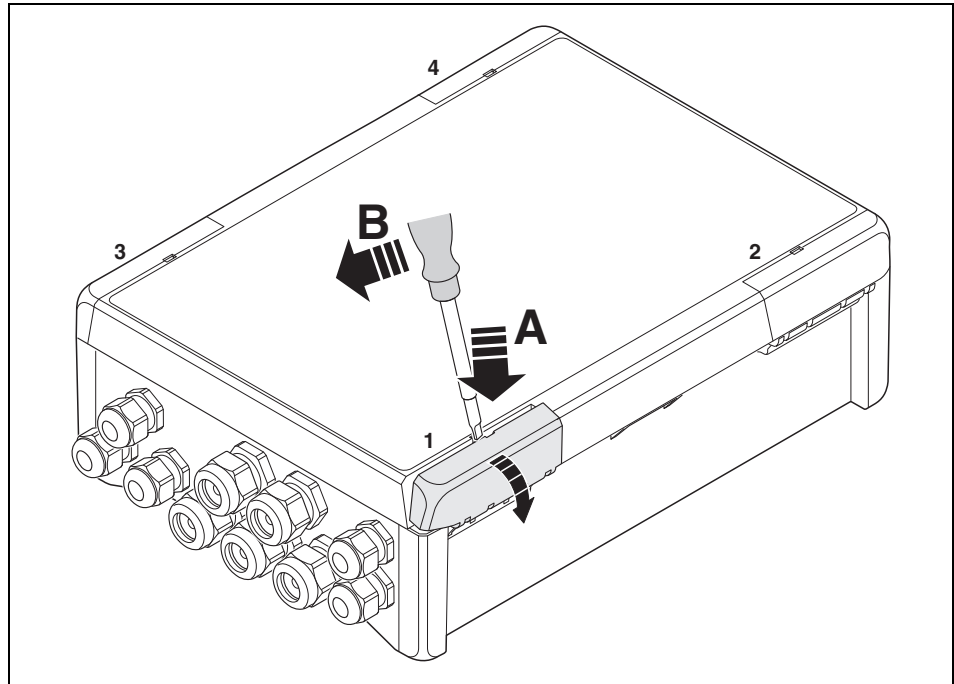


WARNUNG: Gefährliche Berührungsspannung

Öffnen Sie das Gehäuse nur im spannungsfreien Zustand!

- Öffnen Sie das Gehäuse mit einem Schraubendreher.
- Der Türanschlag ist wahlweise links oder rechts (1 + 2 oder 3 + 4).
- Sie können die Tür auch komplett abnehmen.

Bild 3-5 Gehäuse öffnen



4 Installieren

4.1 Montieren und demontieren

**WARNUNG: Gefährliche Berührungsspannung**

Montieren und demontieren Sie die Smart Ethernet Box nur im spannungsfreien Zustand.

**WARNUNG: Absturzgefahr**

- Montieren und demontieren Sie die Smart Ethernet Box ggf. mit zwei Personen.
- Wenn Sie Steig- und Montagehilfen verwenden, z. B. Leitern oder Arbeitsbühnen, beachten Sie die einschlägigen Sicherheitsvorschriften.
- Achten Sie immer auf einen sicheren Stand.

4.1.1 Montageort

Die Smart Ethernet Box ist für die feste Montage im Innen- oder Außenbereich vorgesehen.

- Montieren Sie die Smart Ethernet Box ausschließlich senkrecht und mit den Verschraubungen nach unten.
- Installieren Sie die Smart Ethernet Box in einem nur für befugte Personen zugänglichen Bereich.
- Die Smart Ethernet Box muss im Notfall, zur Bedienung und für Instandhaltungsarbeiten jederzeit frei zugänglich sein.
- Installieren Sie die Smart Ethernet Box an einem Mast oder an einer ebenen, tragfähigen Wand.
- Verwenden Sie geeignetes, dem Untergrund entsprechendes Montagematerial.
- Halten Sie die zulässigen Umgebungsbedingungen ein und beachten Sie das Derating (siehe „[Umgebungsbedingungen](#)“ auf Seite 87). Schützen Sie die Smart Ethernet Box ggf. vor direkter Sonneneinstrahlung.
- Trennen Sie die Smart Ethernet Box räumlich von Frequenzumrichtern, Starkstromgeräten und Wärmequellen. Wärmeentwicklung und Störungen benachbarter Geräte können zu Funktionsausfällen führen.
- Achten Sie bei Arbeiten an der Smart Ethernet Box auf genügend Bewegungsraum. Halten Sie bei Montage, Betrieb und Instandhaltung genügend Platz frei.

4.1.2 Mastmontage

Verwenden Sie zwei Mastschellen für Masten mit einem Durchmesser von 50 mm ... 250 mm (z. B. SCX-CLAMP..., siehe [Seite 81](#)).

- Die gerippte Seite des Montageadapters zeigt auf Sie zu.
 - Innere Öffnungen für Mastdurchmesser 50 ... 90 mm
 - Äußere Öffnungen für Mastdurchmesser 90 ... 250 mm
- Montieren Sie den Montageadapter mit zwei Mastschellen.
- Ziehen Sie die Mastschellen mit dem empfohlenen Drehmoment an (siehe Dokumentation des Herstellers).
- Setzen Sie die Smart Ethernet Box von oben auf den Montageadapter, bis sie sicher einrastet.
- Prüfen Sie den festen Sitz.

Je nach Einsatzort kann es erforderlich sein, die Smart Ethernet Box nach dem Einrasten auszurichten. Ziehen Sie in diesem Fall die Mastschellen nach dem Ausrichten mit dem empfohlenen Drehmoment an.

Bild 4-1 Montageadapter, Mastmontage

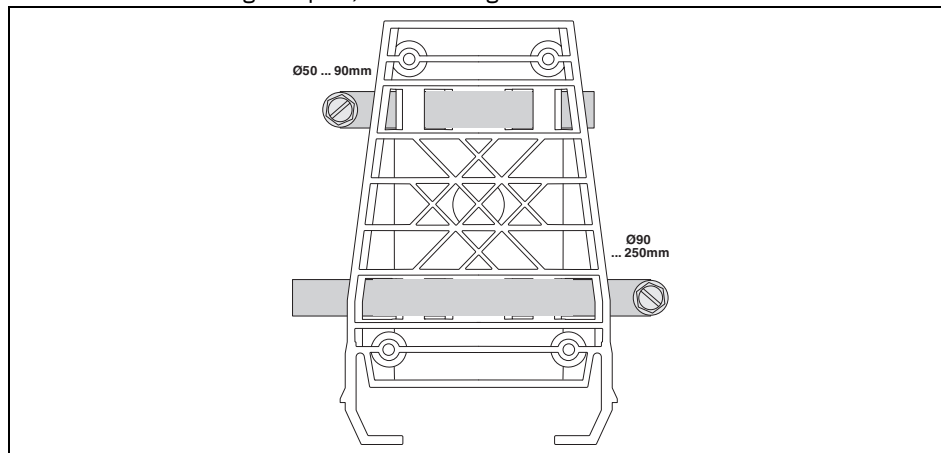
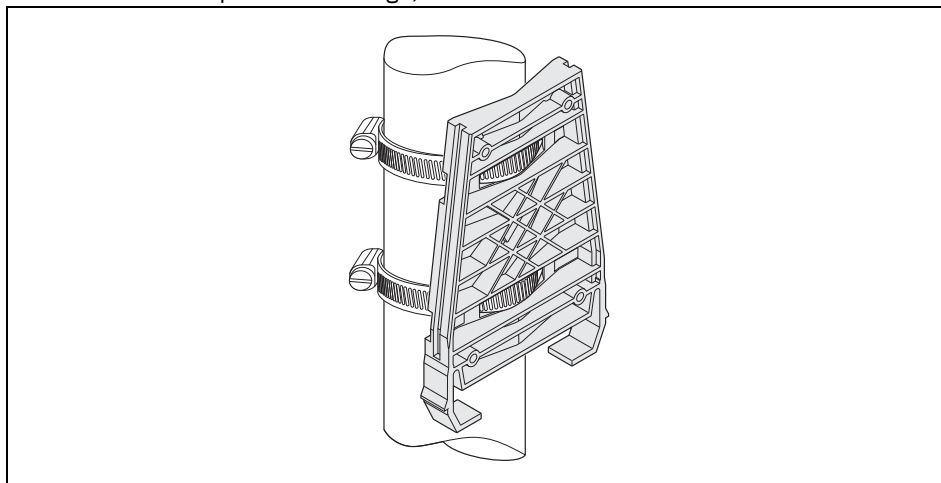


Bild 4-2 Beispiel Mastmontage, Ø 50 ... 90 mm



4.1.3 Wandmontage

Verwenden Sie geeignetes, dem Untergrund entsprechendes Montagematerial.

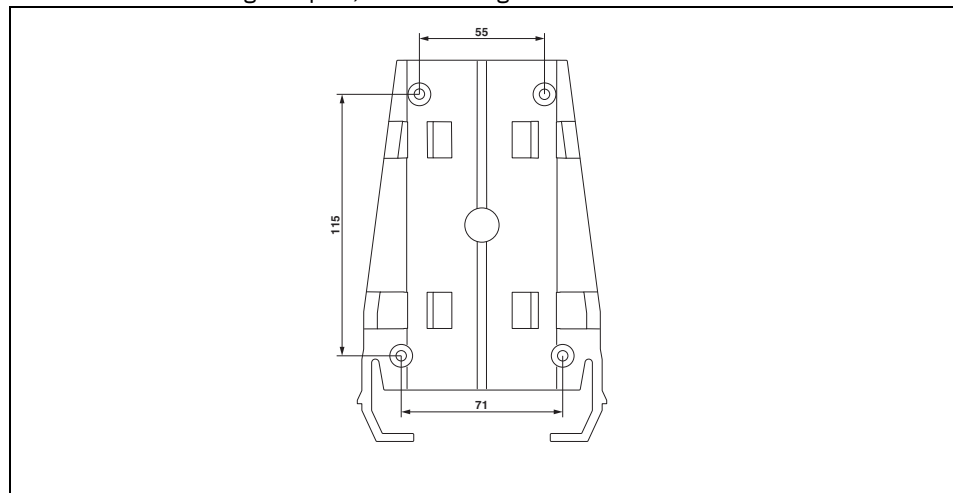
Sie haben zwei Optionen zur Wandmontage:

- Mit dem mitgelieferten Montageadapter, siehe [4.1.3.1](#)
- Über die Befestigungslöcher am Gehäuse, siehe [4.1.3.2](#)

4.1.3.1 Option 1: Montageadapter

- Markieren Sie die Bohrlöcher.
- Bohren Sie die Löcher.
- Die glatte Seite des Montageadapters zeigt auf Sie zu. Befestigen Sie den Montageadapter mit vier Dübeln und Schrauben an der Wand.
 - Schraubenstärke bis Durchmesser 5 mm
 - Schraubenkopf bis Durchmesser 10 mm
 - Sechskantschrauben möglich, bis 8 mm Schlüsselweite (M5)
 - Schlitz- und Kreuzschrauben möglich, bis 10 mm Schraubenkopfgröße (M6)
- Setzen Sie die Smart Ethernet Box von oben auf den Montageadapter, bis sie sicher einrastet.
- Prüfen Sie den festen Sitz.

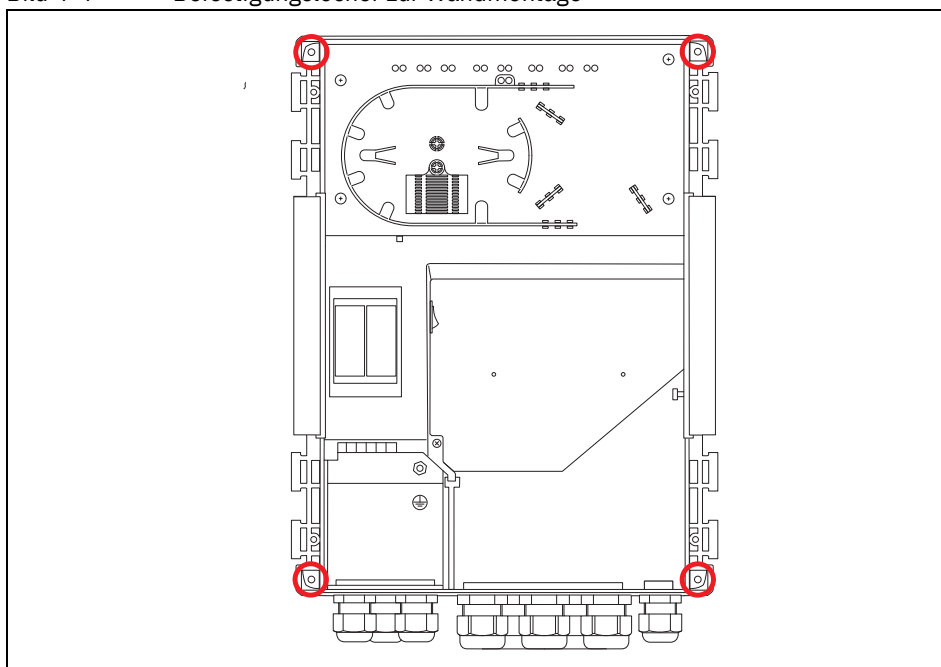
Bild 4-3 Montageadapter, Wandmontage



4.1.3.2 Option 2: Befestigungslöcher am Gehäuse

- Nehmen Sie die Tür des Gehäuses ab (siehe 3.2.5 „Gehäuse öffnen“).
- Markieren Sie die Bohrlöcher.
- Bohren Sie die Löcher.
- Befestigen Sie das Gehäuse mit vier Dübeln und Schrauben an der Wand.
 - Schraubenstärke bis Durchmesser 5 mm
 - Schraubenkopf bis Durchmesser 10 mm
 - Sechskantschrauben nicht möglich
 - Schlitz- und Kreuzschrauben möglich, bis 10 mm Schraubenkopfgröße (M6)
- Prüfen Sie den festen Sitz.
- Montieren Sie die Tür.

Bild 4-4 Befestigungslöcher zur Wandmontage



4.1.4 Gehäuse ab Hardware-Version 21

Ab Hardware-Version 21 bietet das optimierte Gehäuse die folgenden Funktionen:

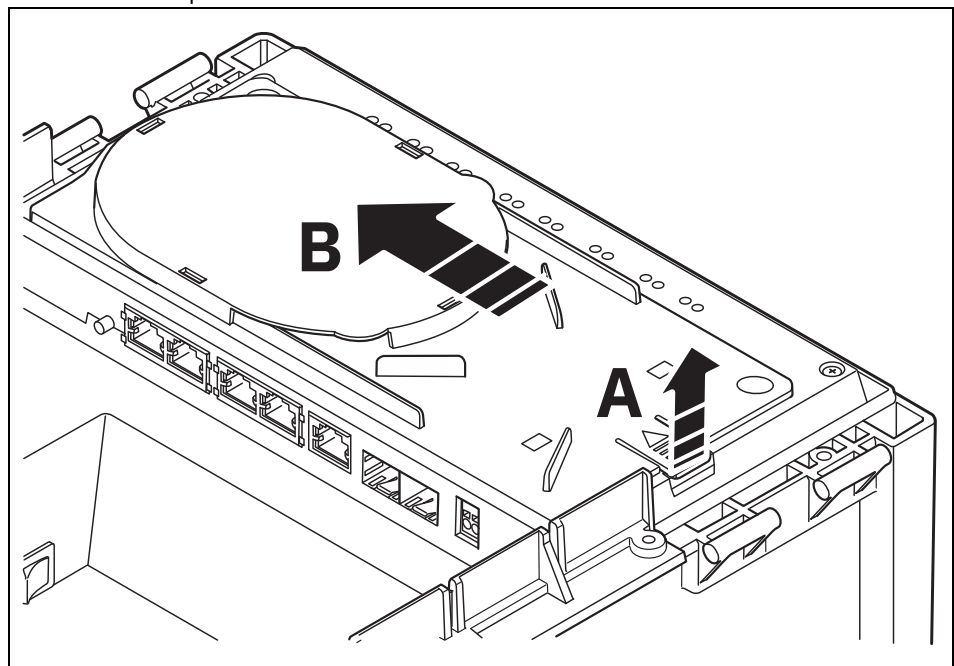
- Herausnehmbare Spleißkassette, siehe [Seite 26](#)
- Herausnehmbare Flanschplatte, siehe [Seite 27](#)
- Erweiterbare Kabelverschraubung für die Versorgungsleitung, siehe [Seite 28](#)

Herausnehmbare Spleißkassette (nur SCX ... 2LX)

Für eine einfache Installation ist die Spleißkassette herausnehmbar.

- Drücken Sie die Rastnase leicht nach oben und schieben Sie die Spleißkassette nach links.
- Entnehmen Sie die Spleißkassette.

Bild 4-5 Spleißkassette entnehmen



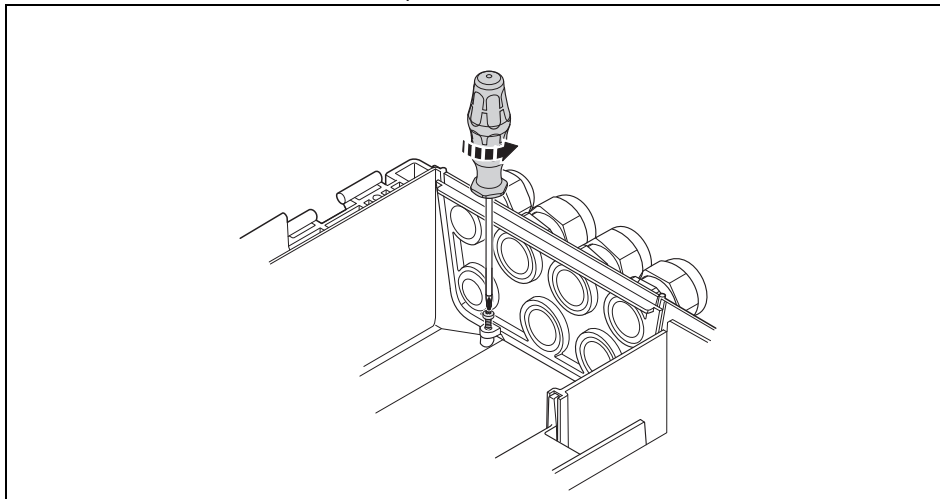
i Ab Hardware-Version 21 enthalten die Geräte SCX ... 2T keine Spleißkassette mehr.

Herausnehmbare Flanschplatte

Die Flanschplatte mit den Kabelverschraubungen ist herausnehmbar.

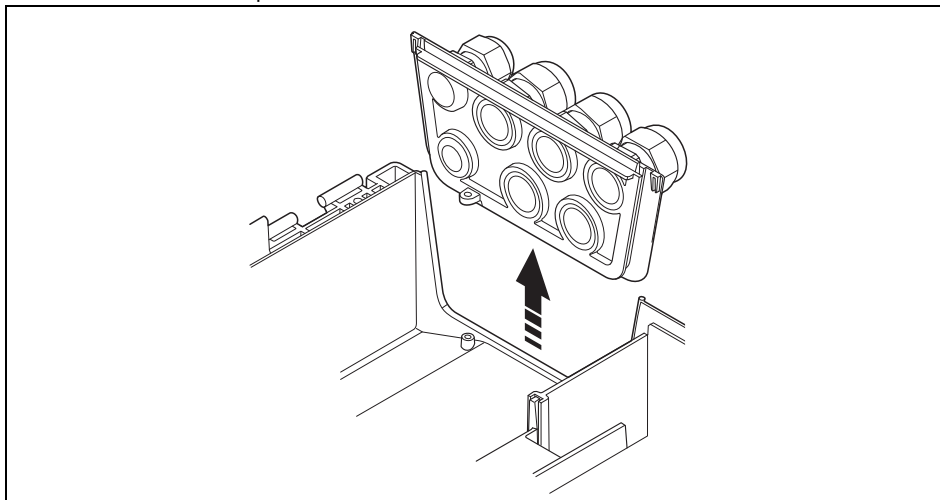
- Lösen Sie die Schraube der Flanschplatte an der Innenseite des Gehäuses.

Bild 4-6 Schraube der Flanschplatte lösen



- Ziehen Sie die Flanschplatte heraus. Achten Sie darauf, dass die Dichtung nicht beschädigt wird.

Bild 4-7 Flanschplatte herausziehen



- Achten Sie beim Wiedereinsetzen der Flanschplatte auf den korrekten Sitz der Dichtung.
- Ziehen Sie die Befestigungsschraube für die Flanschplatte mit maximal 1 Nm an. Die Schraube dient nur zum Fixieren der Flanschplatte, wenn der Deckel geöffnet wird.

Erweiterbare Kabelverschraubung für Versorgungsleitung



ACHTUNG: Gerätebeschädigung

Es ist zulässig, **eine** der Kabelverschraubungen für die Versorgungsleitung auf M32 zu vergrößern. Dies erfolgt auf Verantwortung des Kunden.

- Die zugesicherten Eigenschaften des Geräts, insbesondere zu Dichtigkeit und Schutzart, sind nicht mehr sichergestellt.
- Die Dichtigkeit des Gehäuses muss kundenseitig sichergestellt werden. Beachten Sie die Anwenderdokumentation des Herstellers der Kabelverschraubung.
- Die UL-Zulassung erlischt.

In einigen Anwendungsfällen benötigen Sie eine M32-Kabelverschraubung für die Versorgungsleitung. Es sind aber nur M25-Kabelverschraubungen vormontiert. Deswegen können Sie **eine** der Kabelverschraubungen bei Bedarf auf bis zu M32 vergrößern.

Um Platz zu schaffen, brechen Sie das Schirmblech an der Perforierung ab. Danach können Sie die Bohrung im Gehäuse auf M32 vergrößern.

- Schieben Sie einen Schraubendreher zwischen das Gehäuse und das Schirmblech.
- Um das Schirmblech an der Sollbruchstelle zu brechen, bewegen Sie den Schraubendreher leicht nach außen.
- Bewegen Sie das Schirmblech mit der Hand leicht hin und her, bis es abbricht.
- Entnehmen Sie das abgebrochene Schirmblech.

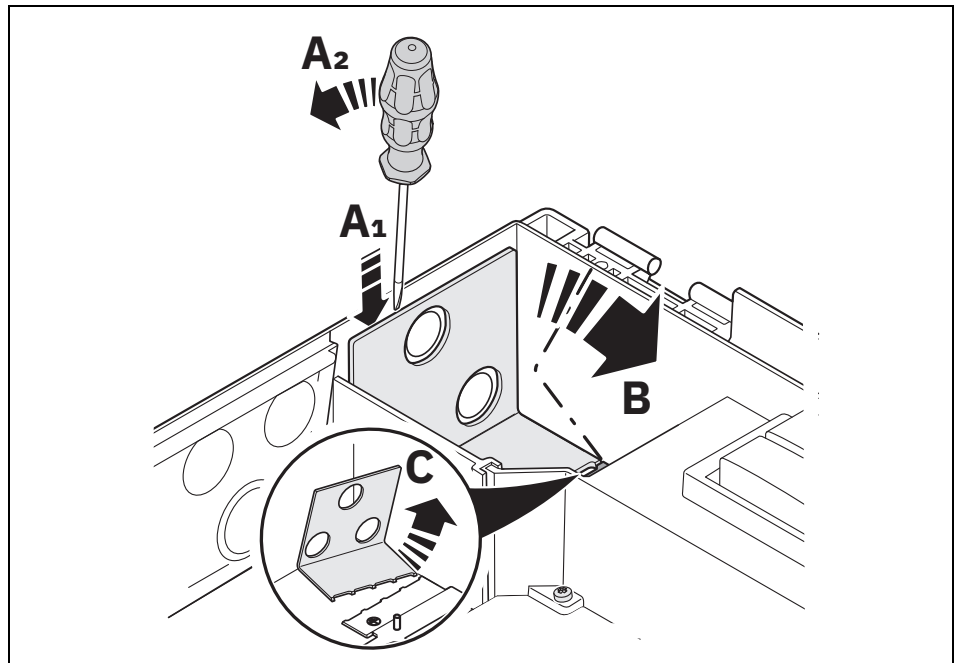


VORSICHT: Verletzungsgefahr

Durch das Herausbrechen des Schirmblechs können scharfe Kanten und Grate entstehen.

- Entgraten Sie ggf. die Kanten der Bruchstelle.

Bild 4-8 Schirmblech herausbrechen



- Vergrößern Sie die Bohrung im Gehäuse.
- Montieren Sie die M32-Kabelverschraubung.

4.1.5 Demontieren

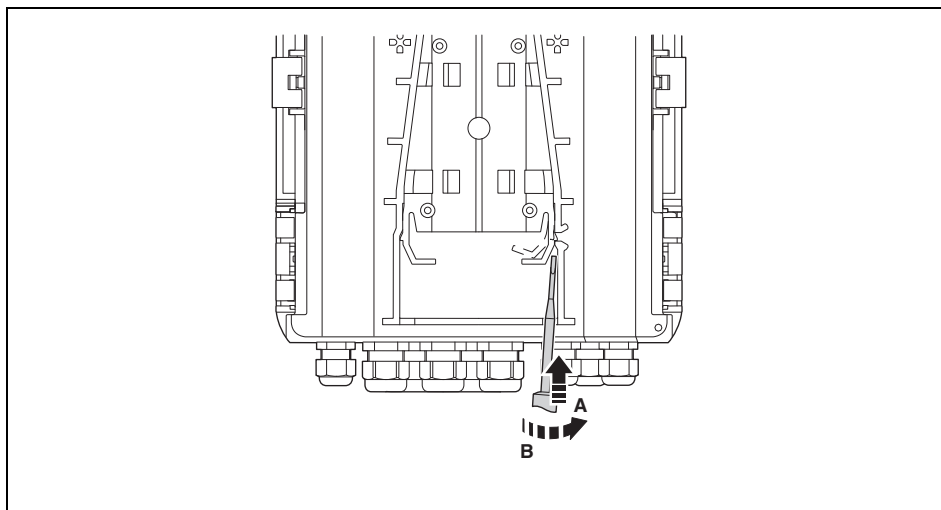


WARNUNG: Gefährliche Berührungsspannung

Demontieren Sie die Smart Ethernet Box nur im spannungsfreien Zustand.

- Stellen Sie sicher, dass die Vorsicherung ausgeschaltet und die Zuleitung spannungsfrei ist.
- Befolgen Sie die fünf Sicherheitsregeln nach EN 50110-1.
- Öffnen Sie das Gehäuse mit einem Schraubendreher.
- Entfernen Sie alle Anschlussleitungen.
- Sichern Sie die Smart Ethernet Box gegen Herunterfallen.
- Führen Sie einen Schraubendreher durch die Öffnung an der Rückseite des Gehäuses ([Bild 4-9](#)).
- Hebeln Sie die Rastnase aus der Verrastung.
- Ziehen Sie die Smart Ethernet Box nach oben.

Bild 4-9 Demontieren



SFP-Module demontieren

Nur SCX 4POE 2LX und SCX 2POE 2LX:

Entnehmen Sie die SFP-Module aus den SFP-Slots (UP1/2).

- Klappen Sie den Ausrasthebel zur Seite und ziehen Sie das SFP-Modul ab (siehe [Bild 4-15](#)).

4.2 Elektrischer Anschluss



WARNUNG: Lebensgefahr durch Stromschlag!

Beim Betrieb können bestimmte Teile der Smart Ethernet Box unter gefährlicher Spannung stehen.

- Sehen Sie in der Nähe der Smart Ethernet Box einen Schalter/Leistungsschalter vor, der als Trennvorrichtung für dieses Gerät gekennzeichnet ist.
- Sehen Sie eine Überstromschutzeinrichtung ($I = 6 \dots 16 \text{ A}$) in der Installation vor.
- Verwenden Sie nur Leitungen, die den vorgeschriebenen Installationsvorschriften hinsichtlich Spannung, Strom, Isolationsmaterial, Belastbarkeit etc. entsprechen.
- Trennen Sie die Smart Ethernet Box bei Wartungsarbeiten von allen Energiequellen. Der Schalter in der Smart Ethernet Box schaltet diese **nicht** spannungsfrei!
- Verbinden oder trennen Sie die Anschlussleitungen niemals unter Last.

Gehen Sie bei Inbetriebnahme- und Wartungsarbeiten nach den fünf Sicherheitsregeln der EN 50110-1 vor:

1. Freischalten
2. Gegen Wiedereinschalten sichern
3. Spannungsfreiheit feststellen
4. Erden und Kurzschließen
5. Benachbarte, unter Spannung stehende Teile abdecken oder abschränken

Nach Abschluss der Arbeiten heben Sie die getroffenen Maßnahmen in der umgekehrten Reihenfolge wieder auf.



ACHTUNG: Elektrostatische Entladung

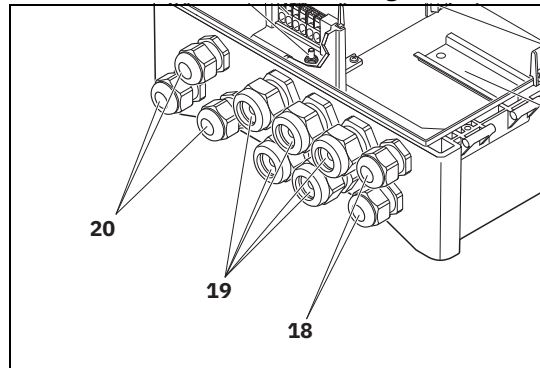
Elektrostatische Entladung kann Bauelemente beschädigen oder zerstören

- Beachten Sie beim Umgang die notwendigen Sicherheitsmaßnahmen gegen elektrostatische Entladung (ESD) nach EN 61340-5-1 und IEC 61340-5-1.

4.2.1 Kabel vorbereiten

- Um einen festen Sitz des Kabels zu gewährleisten, verwenden Sie passende Leiterquerschnitte bzw. Aderendhülsen.

Bild 4-10 Kabelverschraubungen



Pos.	Anschluss		Leiterquerschnitt	Abisolierlänge	Kabeldurchmesser
20	Versorgung	M20	1 ... 6 mm ²	10 mm	6 ... 12 mm
19	Daten	M25	-	-	6 ... 10 mm
18		M20	-	-	6 ... 12 mm

4.2.2 Anschließen der Leitungen

4.2.2.1 Erdung



WARNUNG: Gefährliche Berührungsspannung

- An der PE-Schutzleiterzuleitung kann ein Verschleppungspotenzial auftreten.
- Stellen Sie sicher, dass die Smart Ethernet Box fachgerecht geerdet ist, bevor Sie den PE-Schutzleiter anschließen.
 - Führen Sie die Arbeitsschritte in der hier beschriebenen Reihenfolge aus.
 - Bei Mastmontage: Stellen Sie sicher, dass der Mast geerdet ist.
 - Verbinden Sie eine 6-mm²-Erdungsleitung mit dem geerdeten Mast oder mit dem örtlichen Potenzialausgleich.
 - Verbinden Sie die Erdungsleitung mit der Erdungsschraube.

4.2.2.2 Kabelverschraubungen

 Wenn Sie eine Kabelverschraubung M32 benötigen, beachten Sie auch das Kapitel „Erweiterbare Kabelverschraubung für Versorgungsleitung“.

Führen Sie das Kabel durch die Kabelverschraubung in das Gehäuse.

- Lösen Sie die Überwurfmutter.
- Entnehmen Sie den Dichteinsatz.
- Führen Sie das Kabel durch die Überwurfmutter und den Dichteinsatz.
- Drücken Sie den Dichteinsatz wieder in das Einführungsgewindestück.
- Ziehen Sie die Kabelverschraubungen mit 2 Nm (M20) bzw. 3,5 Nm (M25) an.
- Achten Sie darauf, dass der Dichteinsatz das Kabel dicht umschließt.

Bild 4-11 Kabelverschraubung M20 montieren

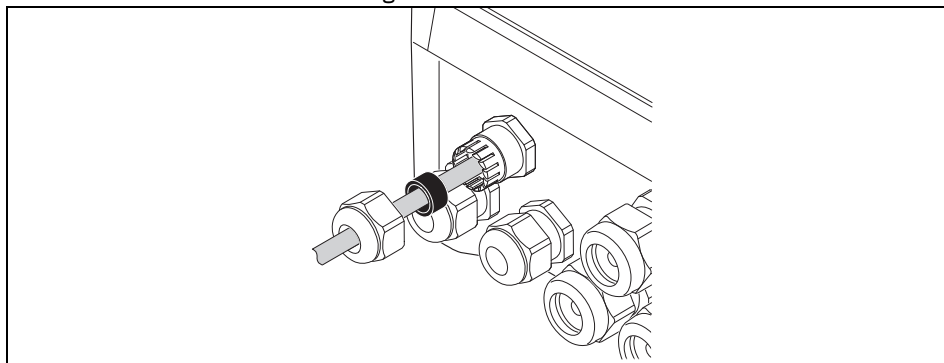
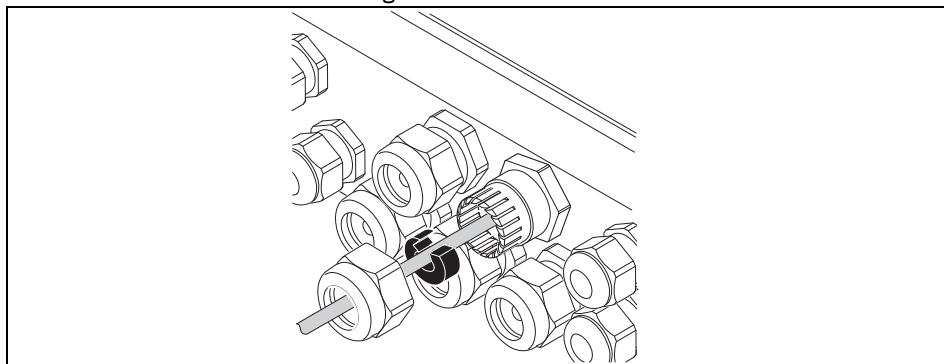


Bild 4-12 Kabelverschraubung M25 montieren



4.2.2.3 Versorgungsspannung

- Stellen Sie sicher, dass die Versicherung ausgeschaltet und die Zuleitung spannungsfrei ist.
- Schließen Sie die Leiter an.
 - L(a) = Außenleiter
 - N(a) = Neutraleiter
 - PE(a) = Schutzleiter



WARNUNG: Gefährliche Berührungsspannung

Die Anschlüsse L(b), N(b) und PE(b) sind für die Versorgung externer Geräte vorgesehen.

- Führen Sie die Versorgungsspannung **nicht** in die Kleinspannungszone innerhalb der Smart Ethernet Box.

Bild 4-13 Versorgungsspannung anschließen

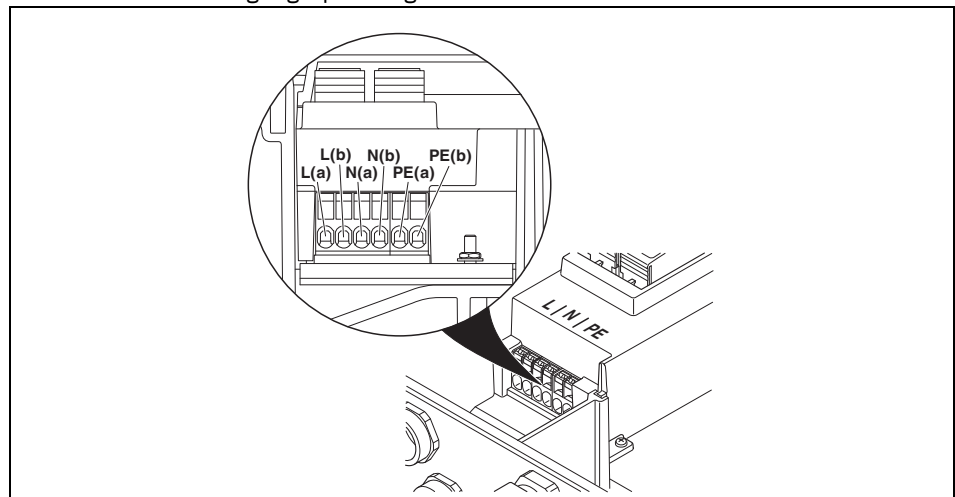
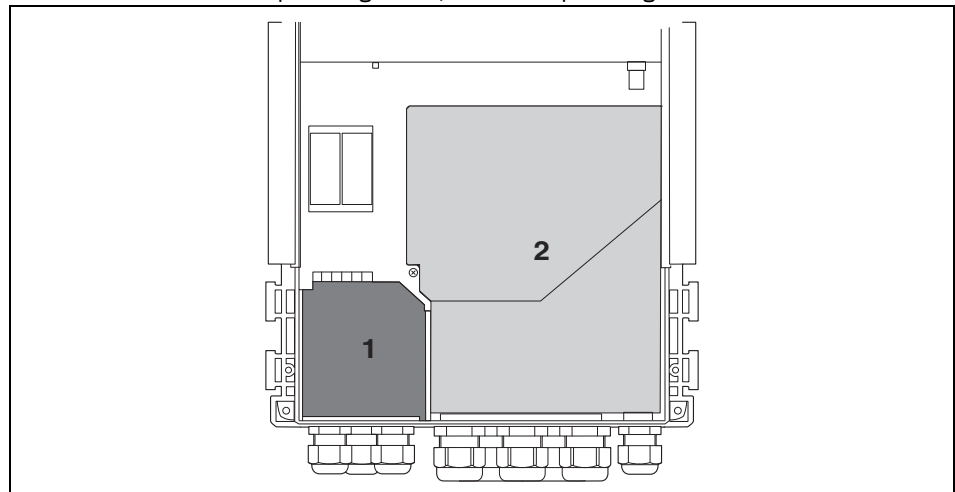


Bild 4-14 1 = Netzspannungszone / 2 = Kleinspannungszone



4.2.2.4 Ethernet-Kabel (PoE)

Verbinden Sie die PoE-Endgeräte mit den PoE-Ports.

- Verwenden Sie ausschließlich geschirmte Twisted-Pair-Kabel und passende abgeschirmte RJ45-Stecker.
- Stecken Sie die Ethernet-Leitung mit dem RJ45-Stecker in die Schnittstelle, bis der Stecker hörbar einrastet.

4.2.2.5 Feldkabel

Bei den Produktvarianten ...2T:

- Schließen Sie das Feldkabel am Uplink-Port an.

Bei den Produktvarianten ...2LX:



ACHTUNG: Fehlfunktion

Zum Verlegen, Anschließen und Verspleißen von Lichtwellenleitern benötigen Sie spezielle Fachkenntnisse. Diese Anleitung setzt Fachkenntnisse im Umgang mit Lichtwellenleitern voraus.

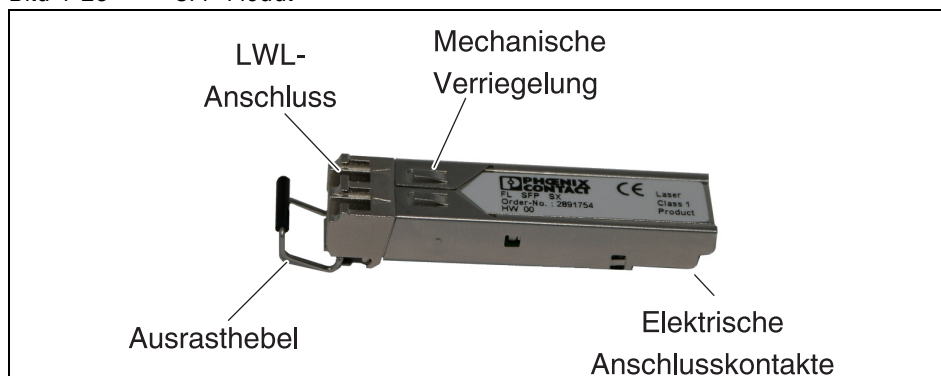


Beachten Sie auch das Kapitel [4.1.4 „Gehäuse ab Hardware-Version 21“](#).

Die SFP-Slots sind zur Aufnahme von SFP-Modulen vorbereitet. SFP-Module sind LWL-Glasfasermodule im SFP-Format. Sie sind separat als Zubehör erhältlich (siehe „Zubehör“).

- Wählen Sie die passenden SFP-Module für Ihren Anwendungsfall.
- Schieben Sie die SFP-Module in die SFP-Slots in der Smart Ethernet Box.
- Achten Sie dabei auf die korrekte mechanische Ausrichtung der SFP-Module.
- Legen Sie den Spleißkamm ein.

Bild 4-15 SFP-Modul



Feldkabel vorbereiten

- Entfernen Sie den Außenmantel und das Aramidgarn auf einer Länge von ca. 1600 mm.
- Führen Sie das Kabel durch die Kabelverschraubung.
- Ziehen Sie die Kabelverschraubung an.
- Entfernen Sie den Mantel der Bündeladern.
- Fixieren Sie die Bündelader mit den mitgelieferten Kabelbindern.

Bild 4-16 LWL-Kabel abmanteln, Kabelverschraubung M20

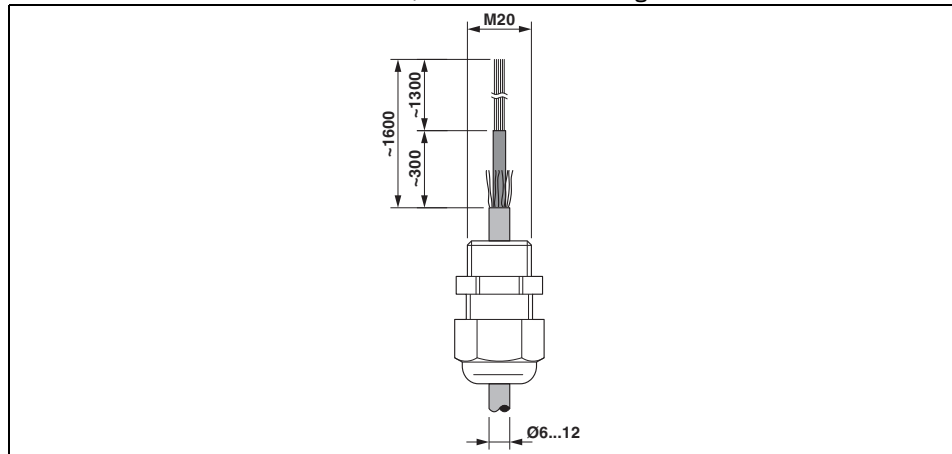
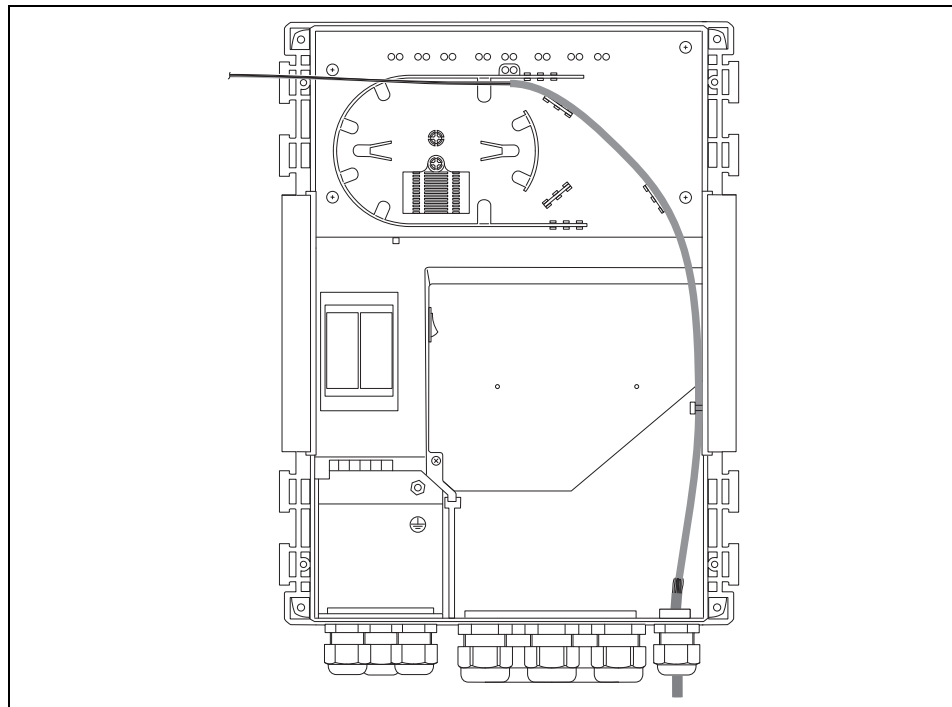
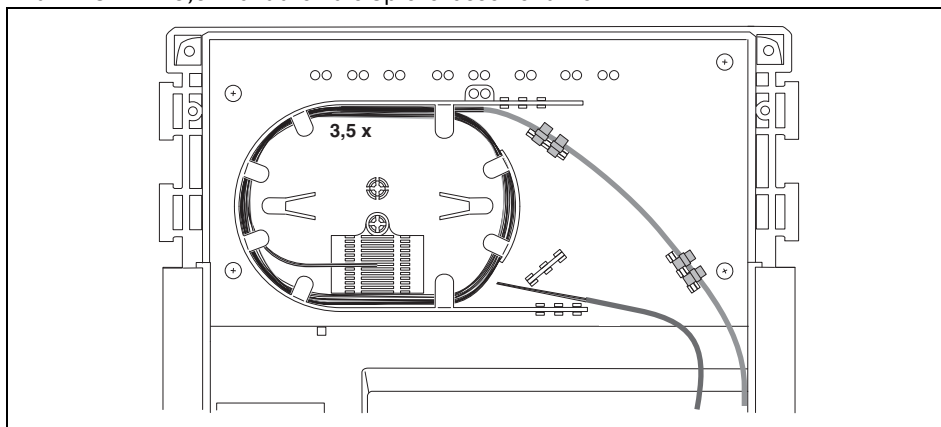


Bild 4-17 LWL-Kabel einführen



- Führen Sie die Fasern ca. 3,5-mal durch die Spleißkassette bis zur Mitte des Spleißkamms.
- Längen Sie die Fasern entsprechend ab.

Bild 4-18 3,5-mal durch die Spleißkassette führen



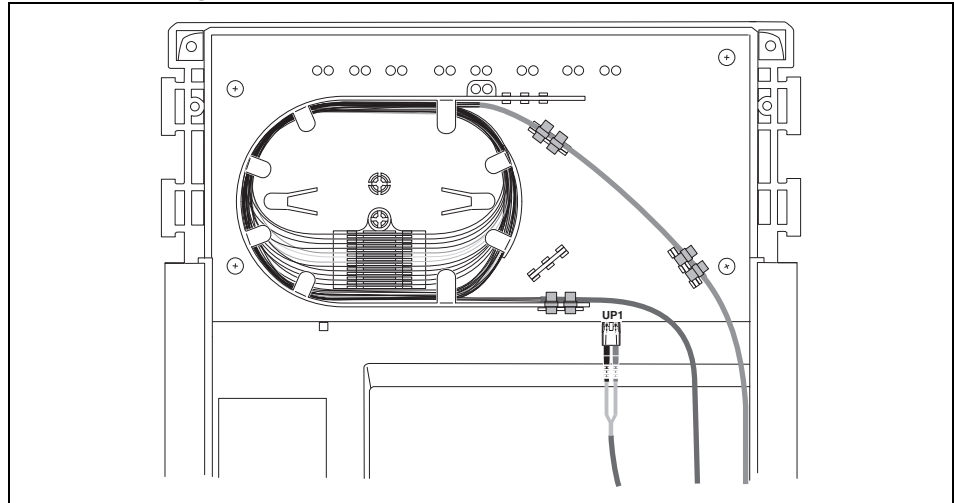
Patch-Kabel vorbereiten

- Verwenden Sie eines der folgenden Patch-Kabel:
 - FOC-LC:PA-LC:PA-OM4:D01/5, 1115621
 - FOC-LC:PA-LC:PA-OS2:D01/5, 1115626
- Trennen Sie das Patch-Kabel in der Mitte durch.
- Entfernen Sie den Außenmantel und das Aramidgarn auf einer Länge von ca. 1400 mm.
- Entfernen Sie den Mantel der Adern auf einer Länge von ca. 1100 mm.
- Fixieren Sie die Adern mit den mitgelieferten Kabelbindern an den entsprechenden Kunststoffstegen.
- Führen Sie die Fasern ca. 3-mal durch die Spleißkassette bis zur Mitte des Spleißkamms.
- Längen Sie die Fasern entsprechend ab.

Verspleißen und Anschließen

- Verspleißen Sie die Fasern in einem Spleißgerät. Beachten Sie die Anwenderdokumentation des Herstellers.
- Führen Sie die verspleißten Fasern durch die Spleißkassette.
- Legen Sie die Spleißschutzhülsen in den Spleißkamm.
- Verrasten Sie die Stecker in den SFP-Modulen.

Bild 4-19 Pigtail anschließen (3-mal durch die Spleißkassette führen)



4.2.3 Zusätzliche Geräte installieren

Auf der Tragschiene in der Smart Ethernet Box können Sie zusätzliche Geräte installieren.



ACHTUNG: Gerätebeschädigung

Beachten Sie beim Installieren zusätzlicher Geräte die folgenden Einschränkungen.

- Versorgen Sie zusätzliche Geräte innerhalb der Smart Ethernet Box ausschließlich über den Schaltausgang (+/-AUX, 24 V DC). Die Gesamtausgangsleistung der PoE-Ports reduziert sich dadurch um 10 W.
 Ⓛ **ACHTUNG:** Der Schaltausgang ist **nur** für die Versorgung von Geräten innerhalb der Smart Ethernet Box vorgesehen.
- Die Gesamtleistung der zusätzlichen Geräte darf 10 W nicht überschreiten.
- Verwenden Sie die angegebenen Leiterquerschnitte und Abisolierlängen für den 24-V-Ausgang (siehe „Schaltausgang“).
- Wenn Sie zusätzliche Geräte installieren, kann die CE-Konformität der Smart Ethernet Box beeinflusst werden. Ggf. müssen Sie die CE-Konformität neu betrachten.

4.3 Inbetriebnahme

Kabelführung

- Kontrollieren Sie die Kabelführung und die Biegeradien. Um Beschädigungen der Kabel zu vermeiden, stellen Sie sicher, dass die Kabel nicht zu stark geknickt sind.

Blindstopfen

- Verschließen Sie ungenutzte Kabelverschraubungen mit den mitgelieferten Blindstopfen.
 - Die großen Blindstopfen sind für die Kabelverschraubungen M20 vorgesehen.
 - Die kleinen Blindstopfen sind für die Kabelverschraubungen M25 vorgesehen.
- Ziehen Sie die ungenutzten Kabelverschraubungen zunächst nur lose an.
- Drücken Sie den Blindstopfen in den Dichteinsatz.

Kabelverschraubungen anziehen

- Prüfen Sie den festen Sitz und die Dichtigkeit aller Kabelverschraubungen. Ziehen Sie lose Verbindungen unter Berücksichtigung des Drehmoments fest.
 - 2 Nm (M20)
 - 3,5 Nm (M25)

Leitende Verbindungen

- Prüfen Sie vor dem Herstellen der Versorgungsspannung alle leitenden Verbindungen.
- Wenn die Smart Ethernet Box fachgerecht angeschlossen ist, schalten Sie die Versicherung ein.



Das Konfigurieren der Smart Ethernet Box wird in [Kapitel 5, „Konfigurieren“](#) beschrieben.

4.3.1 Gehäuse schließen

- Achten Sie darauf, dass sich keine Fremdkörper zwischen der Türdichtung und dem Gehäuse befinden.
- Verriegeln Sie die Tür.
- Um die Smart Ethernet Box vor unbefugtem Zugriff zu schützen, können Sie die Tür zusätzlich mit einem Vorhängeschloss sichern.
 - Ein Türriegel mit Verriegelungslasche ist als Zubehör erhältlich (SCX-DOOR-LOCK, 1184401).
 - Das Vorhängeschloss ist nicht im Lieferumfang enthalten. Sie benötigen ein Vorhängeschloss mit einer Bügelstärke bis 12 mm.

Bild 4-20 SCX-DOOR-LOCK: Verriegelungslasche einhängen

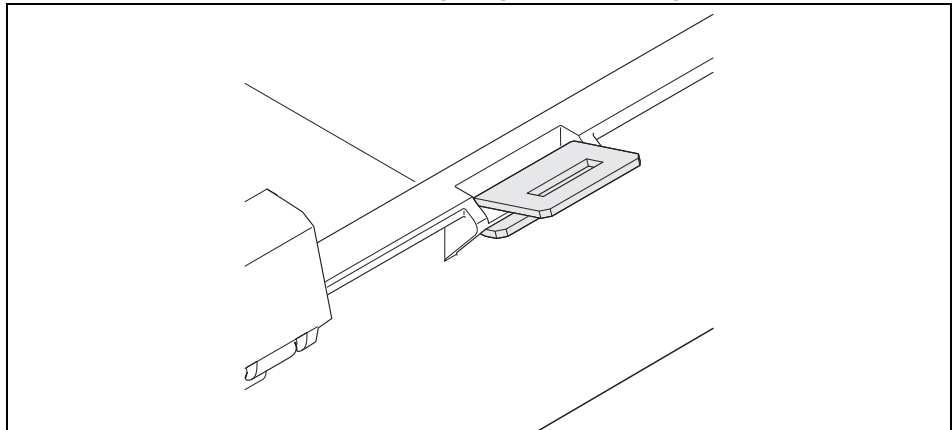
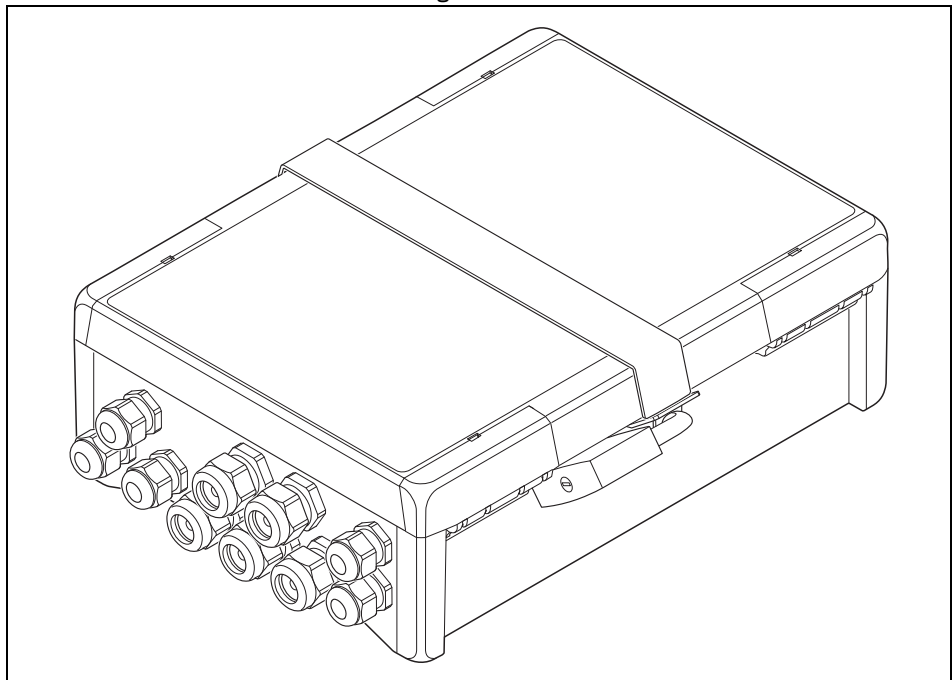


Bild 4-21 SCX-DOOR-LOCK: Türriegel montieren



5 Konfigurieren

5.1 Web-based Management

Durch das neue Responsive Design ist das Web-based Management auch auf mobilen Geräten wie Smartphones oder Tablets komfortabel zu bedienen.

Voraussetzungen

- Die Smart Ethernet Box muss an die Spannungsversorgung angeschlossen sein.
- Der Rechner, mit dem Sie die Konfiguration vornehmen, muss mit der Smart Ethernet Box verbunden sein:
 - Vor Ort über den lokalen Konfigurations-Port
 - Oder
 - Aus der Ferne über die Uplink-Ports
- Der Rechner muss sich im selben Netzwerkbereich befinden.
- Auf dem Rechner ist ein Browser installiert. Das Web-based Management wurde getestet mit Google Chrome®.

Web-based Management starten

- Verbinden Sie einen Rechner mit der Smart Ethernet Box.
- Die IP-Adresse wird automatisch über DHCP vergeben. Im Auslieferungszustand ist auf dem Gerät der DHCP-Client aktiviert. Die dem Gerät zugewiesene IP-Adresse entnehmen Sie dem DHCP-Server.

Wenn Sie kein DHCP verwenden, stellen Sie die feste IP-Adresse über den Mode-Taster ein (siehe [5.2 „Mode-Taster“](#)).

- Passen Sie bei Bedarf die IP-Parameter des Rechners an.
- Öffnen Sie auf dem Rechner einen Browser.
- Geben Sie die IP-Adresse im Adressfeld Ihres Browsers ein.
- Zum Einloggen benötigen Sie den Benutzernamen und das Passwort.
 - Benutzername: admin (Default)
 - Passwort: private (Default)

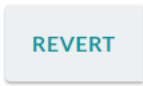
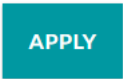


ACHTUNG: Netzwerksicherheit

Ändern Sie bei der ersten Konfiguration das Passwort (siehe [„Basic Setup“](#)).

5.1.1 Schaltflächen Revert, Apply und Save

Tabelle 5-1 Revert, Apply, Save

Schaltfläche	Funktion
	Die Änderungen auf der Webseite werden wieder zurückgesetzt.
	Die geänderten Parameter werden auf das Gerät übertragen. ⓘ ACHTUNG: Die Änderungen sind noch nicht dauerhaft gespeichert. Bei einem Neustart des Geräts gehen sie wieder verloren.
	Die Änderungen werden dauerhaft gespeichert.

5.1.2 Basic Setup

Bild 5-1 Basic Setup

Basic Setup

IP Address Assignment	STATIC ▼ ⓘ
IP Address	Please enter 172.22.2.200 ⓘ
Network Mask	Please enter 255.255.0.0 ⓘ
Default Gateway	Please enter 0.0.0.0 ⓘ

Basic Setup		
IP Address Assignment	STATIC	Statische IP-Adresse manuell eingeben
	BOOTP	IP-Adressvergabe über BootP
	DHCP	IP-Adressvergabe über DHCP, Auslieferungszustand
IP Address	nur im STATIC-Modus:	
Network Mask	Statische IP-Adresse, z. B. 192.168.0.254	
Default Gateway	Netzmaske, z. B. 255.255.255.0	
	Standard-Gateway, z. B. 192.168.0.1	
User Password	ⓘ ACHTUNG: Ändern Sie aus Sicherheitsgründen bei der ersten Konfiguration das Passwort. 8 ... 64 Zeichen, erlaubte Zeichen: A...Z, a...z, 0...9	
Retype Password		
Network Time Protocol	Unicast	Aktivieren Sie die Synchronisierung mit einem SNTP-Zeit-Server.
	Broadcast	
Primary SNTP Server	IP-Adresse des primären oder sekundären SNTP-Servers	

5.1.3 Administration

5.1.3.1 User Accounts

Wenn Sie Administratorrechte haben, können Sie hier Nutzer hinzufügen, bearbeiten oder löschen.

Bild 5-2 User Accounts, Add User

Add User

User Name

Please enter User

User Role

Admin

Maximum Failed Logins

Please enter 5

Login Block Time [min]

Please enter 1

User Password

Please enter

Retype Password

Please enter

Administration, User Management, Add User		
User Name	Name des neuen Nutzers	
User Role	Wählen Sie eine Nutzerrolle.	
	Admin	Administrator, vollständige Schreib- und Leserechte, anlegen und verwalten neuer Nutzer
	Expert	Lese- und Schreibrechte, keine Nutzerverwaltung
	Read-only	Nur Leserechte
	...	Sie können auch selbst weitere Nutzerrollen definieren, siehe Kapitel „User Roles“ auf Seite 45 .
Maximum Failed Logins	Maximale Anzahl an fehlgeschlagenen Logins. Danach wird der Nutzer für eine definierte Zeit gesperrt (Login Block Time).	
Login Block Time [min]	Nach Ablauf dieser Zeit darf der Nutzer sich wieder einloggen.	
User Password	ⓘ ACHTUNG: Ändern Sie aus Sicherheitsgründen bei der ersten Konfiguration das Passwort.	
Retype Password		
	8 ... 64 Zeichen, erlaubte Zeichen: A...Z, a...z, 0...9	

5.1.3.2 User Roles

Wenn Sie Administratorrechte haben, können Sie hier Nutzerrollen neu anlegen, bearbeiten und löschen.

Bild 5-3 User Roles, Add Role

Add Role

Role Name

Please enter Role

Privilege	RO	RW
System Configuration	☐	☐
Device Identification	☐	☐
User Management	☐	☐
Network	☐	☐
User Interface Configuration	☐	☐
Device Discovery	☐	☐
L2 and L3 Communication	☐	☐

Administration, User Roles, Add Role

Role Name	Name der neuen Nutzerrolle	
Privilege	Vergeben Sie Rechte für die neue Nutzerrolle.	
	RO	Nur Leserechte
	RW	Lese- und Schreibrechte

5.1.3.3 Time Settings

Bild 5-4 Time Settings

Manual Time Set	
Current System Time	2022/08/30 08:52:09 
Local Time with UTC Offset and DST Time Shift	2022/08/30 09:52:09 
Manual Time Set in UTC	Please choose  
UTC Offset	+01h (Berlin, Paris)  

Administration, Time Settings		
Current System Time	Aktuelle Systemzeit in UTC	
Local Time with UTC Offset and DST Time Shift	Aktuelle, lokale Zeit unter Berücksichtigung der angegebenen Zeitzone und Sommer-/Winterzeitumstellung	
Manual Time Set in UTC	Falls kein SNTP-Server verfügbar ist, geben Sie die Zeit manuell ein.  Das Gerät hat keine batteriegepufferte Echtzeituhr. Bei manueller Zeiteingabe kann es nach einem Gerätestart zu Abweichungen in der Uhrzeit kommen.	
UTC Offset	Bei Zeitinformation, z. B. in der Event-Tabelle, wird die Greenwich Mean Time (GMT, Winter) angegeben. Die lokale Zeit berechnet sich aus der Systemzeit und dem UTC-Offset. – Wählen Sie Ihre Zeitzone. Beachten Sie ggf. die Umstellung zwischen Sommer- und Winterzeit.	
Daylight Saving Mode	Wählen Sie die Sommer-/Winterzeitumstellung.	
	Manual Standard Time	Keine Umstellung zwischen Sommer- und Winterzeit
	Manual Daylight Saving Time	Manuelles Umstellen zwischen Sommer- und Winterzeit
	Automatic - Rule Based	Automatisches Umstellen zwischen Sommer- und Winterzeit – Definieren Sie die Regeln für das automatische Umstellen. – Wählen Sie eine Regel, Monat, Tag und Uhrzeit, jeweils für Start und Ende der Sommerzeit (Daylight Saving Time).
Network Time Protocol	Unicast	Aktivieren Sie die Synchronisierung mit einem SNTP-Zeit-Server.
	Broadcast	
Primary SNTP Server	IP-Adresse des primären oder sekundären SNTP-Servers	
Secondary SNTP Server		

Administration, Time Settings	
Primary Server Description	Beschreibung des primären oder sekundären SNTP-Servers
Secondary Server Description	
Synchronization Status	Status der Synchronisierung
Last SNTP Synchronization	

5.1.3.4 Device Access

Bild 5-5 Device Access

Device Access

Web Server Mode

HTTP

⌵ ⓘ

Welcome Page

Enabled

⌵ ⓘ

Logout Timeout [s]

Please enter
3600

ⓘ

CLI Service

Telnet

⌵ ⓘ

MD5 Hash of SSH Hostkey

ed:aa:54:99:4f:e9:a6:ec:42:b6:c5:5d:0e:0e:af:cc

ⓘ

Administration, Device Access		
Web Server Mode	Disabled	Sie deaktivieren die Webschnittstelle. ⓘ ACHTUNG: Datenverlust Sie haben keinen Zugriff mehr auf das Web-based Management. Sie können das Gerät nur noch über SNMP oder die Kommandozeile (Command Line Interface, CLI) konfigurieren. Wenn diese Funktionen deaktiviert sind, ist kein Zugriff mehr möglich. Sie müssen das Gerät auf Werkseinstellungen zurücksetzen.
	HTTP	Standard, unsicher
	HTTPS	Sichere Verbindung
Welcome Page	Enabled	Beim Login wird die Willkommensseite angezeigt.
	Disabled	Beim Login werden nur die Felder für den Nutzernamen und das Passwort angezeigt. Die Seite ist neutral.
Logout Timeout (seconds)	Zeit, nach der ein inaktiver Nutzer automatisch ausgeloggt wird, 180 ... 3600 Sekunden	

Administration, Device Access		
CLI Service	Disabled	Keine Eingabe über Command Line Interface
	Telnet	Command Line Interface über Telnet oder SSH
	SSH	
MD5 Hash of SSH Hostkey	MD5-Hash-Wert während einer SSH-Verbindung	
Smart Mode Button	Disabled: Um erhöhte Sicherheitsanforderungen zu erfüllen, können Sie den Mode-Taster am Gerät deaktivieren. Informationen zum Mode-Taster finden Sie im Kapitel 5.2 . ⓘ ACHTUNG: Funktionsverlust Wenn Sie den Mode-Taster deaktivieren, stehen einige Backup-Funktionen nicht mehr zur Verfügung, z. B. das Einstellen einer statischen IP-Adresse.	
Create New Context	ⓘ Um HTTPS- und SSL-Funktionen nutzen zu können, erstellen Sie zuerst den Sicherheitskontext. Der Sicherheitskontext enthält alle Zertifikate für HTTPS- und SSL-Verbindungen zum Gerät. Es kann einige Minuten dauern, bis der Sicherheitskontext erstellt ist.	
Current State	Verfügbarkeit des Sicherheitskontexts	
Status	Status des Sicherheitskontext-Uploads	
Choose Upload File	Wählen Sie die Upload-Datei. Der Dateiname darf keines der folgenden Zeichen enthalten: / \ < > : ? * Leerzeichen	
Download Security Context File	Der aktuelle Sicherheitskontext (HTTPS- und SSH-Zertifikate) wird in eine Datei geschrieben. Diese Datei können Sie später in eine andere Smart Ethernet Box hochladen.	
Root CA	Wenn Sie auf „cacert.cet“ klicken, wird das Root-CA-Zertifikat für die Installation in den Browser geladen.	

5.1.3.5 Reboot Device & Factory Defaults

Bild 5-6 Reboot Device & Factory Defaults

Reboot Device

Reboot Device

REBOOT ⓘ

Factory Default

Factory Default

SET FACTORY DEFAULT ⓘ

Administration, Reboot Device & Factory Defaults	
Reboot Device	ⓘ ACHTUNG: Neustart, alle nicht gespeicherten Änderungen gehen verloren!
Factory Default	ⓘ ACHTUNG: Zurücksetzen auf Werkseinstellungen, alle Änderungen gehen verloren!

5.1.3.6 Device Identification

Bild 5-7 Device Identification

Device Identification	
Device Name	Please enter SMARTCAMERABOX i
Device Description	Please enter Airport surveillance i
Physical Location	Please enter Gate 21 check-in i
Device Contact	Please enter Video Surveillance Mr Bob Builder i

Administration, Device Identification	
Device Name	Geben Sie Informationen zum Gerät ein.
Device Description	
Physical Location	
Device Contact	

5.1.3.7 RADIUS Authentication

RADIUS (Remote Authentication Dial-in User Service) ist ein Client-Server-Protokoll zur Authentifizierung von Teilnehmern/Benutzern (Supplikanten) bei Einwählverbindungen.

- Der **RADIUS-Server** ist im geschützten Netzwerk installiert. Er ist ein zentraler Authentifizierungsserver. Geräte und Dienste (Authenticators) wenden sich an den RADIUS-Server, um Passwörter der Teilnehmer/Benutzer prüfen zu lassen. Die Teilnehmer/Benutzer kennen das eigentliche Passwort nicht, dieses ist nur dem Authenticator und dem RADIUS-Server bekannt.
- Der **Authenticator** prüft die vom einwählenden Teilnehmer übermittelten Authentifizierungsinformationen. Er gewährt oder verhindert den Zugriff auf das LAN oder VLAN. Für einwählende Teilnehmer ist der Authenticator ein Server.

Bild 5-8 RADIUS Authentication

Global Radius Authentication Server Configuration

Dot1x Authenticator	Enabled  
Radius Server IP Address	Please enter 0.0.0.0 
Radius Server Port	Please enter 1812 
Radius Shared Secret	Please enter 

Administration, RADIUS Authentication		
Dot1x Authenticator	Disabled	Kein 802.1x-Authenticator
	Enabled	Das Gerät ist ein 802.1x-Authenticator.
Radius Server IP Address	IP-Adresse des RADIUS-Servers	
Radius Server Port	UDP-Port des RADIUS-Servers	
Radius Shared Secret	Geben Sie das Shared Secret für die verschlüsselte Kommunikation mit dem RADIUS-Server ein. – Maximal 128 Zeichen – Buchstaben, Ziffern und folgende Sonderzeichen: \$%&@\()?=[{}]*-_<>#^.,:~	
Dot1x Port Configuration Table	Name	Pro Port kann ein Endgerät über 802.1x authentifiziert werden.
	Authentication Mode	Auto: An dem Port angeschlossene Geräte werden über 802.1x authentifiziert (nur wenn Dot1x Authenticator aktiviert ist). Force Authenticate: Alle an dem Port angeschlossenen Geräte werden authentifiziert. Force Unauthenticate: Kein an dem Port angeschlossenes Gerät wird authentifiziert.
	Re-Authentication Mode	Disabled: Keine erneute Authentifizierung Enabled: Regelmäßige erneute Authentifizierung
	Re-Authentication Period (secs)	Regelmäßige erneute Authentifizierung des Teilnehmers im angegebenen Intervall, 1 ... 65535 Sekunden

5.1.3.8 Syslog

Bild 5-9 Syslog

Syslog

Syslog Status

Enabled

▼ ⓘ

Syslog Server 1

Please enter 0.0.0.0

ⓘ

Syslog Server 1 Port

Please enter 514

ⓘ

Syslog Server 2

Please enter 0.0.0.0

ⓘ

Syslog Server 2 Port

Please enter 514

ⓘ

Administration, Syslog		
Syslog Status	Disabled	Keine Kommunikation zu einem syslog-Server
	Enabled	Kommunikation zu einem syslog-Server
Syslog Server 1 Syslog Server 2	Geben Sie die IP-Adresse des syslog-Servers ein.	
Syslog Server 1 Port Syslog Server 2 Port	UDP-Port des syslog-Servers Werkseinstellung: 514	
Syslog Test Message	Senden Sie eine Testnachricht an den syslog-Server.	
Message Group	Wählen Sie eine oder mehrere Nachrichtengruppen, die zum syslog-Server gesendet werden.	

5.1.3.9 Config Up/Download

Bild 5-10 Config Up/Download

Config Upload

Note: The new configuration will become active after the device was restarted manually, this should not be done before the status is successful.

Status

No transfer started

Choose upload file

Datei auswählen

Keine ausgewählt

START UPLOAD

Administration, Config Up/Download	
Status	Status beim Hochladen einer Konfiguration Wenn die Datei vollständig hochgeladen ist (Status: Successful), können Sie das Gerät manuell neu starten. Die neue Konfiguration ist erst nach dem Neustart aktiviert.
Choose Upload File	Der Dateiname darf keines der folgenden Zeichen enthalten: / \ < > : ? * Leerzeichen
Download Config File	Die aktuelle Konfiguration wird heruntergeladen und in eine Datei geschrieben.

5.1.3.10 **Firmware Update**

Bild 5-11 Firmware Update

Reboot after firmware update	Reboot ▼ i
Choose update file	Datei auswählen Keine ausgewählt i
Last Update Status	--- i

Administration, Firmware Update		
Reboot After Firmware Update	Reboot	Neustart nach dem Firmware-Update
	No Reboot	Kein Neustart nach dem Firmware-Update Die neue Firmware wird beim nächsten Neustart aktiviert.
Choose Update File	Der Dateiname darf keines der folgenden Zeichen enthalten: / \ < > : ? * Leerzeichen	
Last Update Status	Status des Firmware-Updates ⓘ ACHTUNG: Während des Updates muss die Smart Ethernet Box mit der Versorgungsspannung verbunden bleiben.	

5.1.4 Configuration

5.1.4.1 Network

Bild 5-12 Network

Network

IP Address Assignment

STATIC

IP Address

Please enter
192.168.0.61

Network Mask

Please enter
255.255.0.0

Default Gateway

Please enter
0.0.0.0

Configuration, Network		
IP Address Assignment	STATIC	Statische IP-Adresse manuell eingeben
	BOOTP	IP-Adressvergabe über BootP
	DHCP	IP-Adressvergabe über DHCP, Auslieferungszustand
IP Address	nur im STATIC-Modus:	
Network Mask	Statische IP-Adresse, z. B. 192.168.0.254	
Default Gateway	Netzmaske, z. B. 255.255.255.0	
	Standard-Gateway, z. B. 192.168.0.1	
ACD Mode	Durch Fehlkonfiguration kann es dazu kommen, dass mehrere Teilnehmer im Netzwerk dieselbe IP-Adresse nutzen. Das führt zu Problemen im gesamten Netzwerk. Wenn Sie den ACD-Mode aktivieren, wird dieses erfasst. Der Teilnehmer wird über die MAC-Adresse angezeigt. Die Änderungen werden erst nach einem Neustart übernommen.	
	None	Kein Address Conflict Detection
	ACD	Address Conflict Detection aktiv

5.1.4.2 Ports

Bild 5-13 Ports

Ports							
Name ¹	Status	Mode	Jumbo Frames	MTU [byte]	Default Priority ¹	Flow Control	
UP1	Enabled ▾	Auto ▾	Disabled ▾	1536	0 ▾	Disabled ▾	
UP2	Enabled ▾	Auto ▾	Disabled ▾	1536	0 ▾	Disabled ▾	
CONF	Enabled ▾	Auto ▾	Disabled ▾	1536	0 ▾	Disabled ▾	
POE1	Enabled ▾	Auto ▾	Disabled ▾	1536	0 ▾	Disabled ▾	
POE2	Enabled ▾	Auto ▾	Disabled ▾	1536	0 ▾	Disabled ▾	
POE3	Enabled ▾	Auto ▾	Disabled ▾	1536	0 ▾	Disabled ▾	
POE4	Enabled ▾	Auto ▾	Disabled ▾	1536	0 ▾	Disabled ▾	

Configuration, Ports

Ports	Name	Port
	Status	Disabled: Port deaktiviert Enabled: Port aktiv
	Mode	Übertragungsmodus und -geschwindigkeit ¹ Wenn Sie „Fast Startup“ wählen, müssen Sie RSTP unter „Network Redundancy“ deaktivieren. Nur so erreichen Sie einen schnellen Link-Aufbau.
	Jumbo Frames	Disabled: Keine Unterstützung von Jumbo Frames Enabled: Unterstützung von Jumbo Frames (>1518 Bytes), MTU automatisch auf 9600 Byte eingestellt
	MTU [byte]	Maximum Transmission Unit, 1522 ... 9600 Byte
	Default Priority	Priorität für ankommende Datenpakete auf diesem Port, wenn sie nicht schon eine Priorität in Form eines Tags enthalten
	Flow Control	Disabled: Keine Datenflusssteuerung Enabled: Datenflusssteuerung für eine möglichst kontinuierliche Datenübermittlung ohne Verluste

5.1.4.3 Port Mirroring

Über Port-Mirroring können Sie den ein- und ausgehenden Datenverkehr auf den gewählten Ports beobachten. Kopien der Frames werden an den Ziel-Port gesendet, wo sie z. B. aufgezeichnet werden können.

Bild 5-14 Port Mirroring

Port Mirroring

Global Status

Disabled

▼ ⓘ

Destination Port

UP1

▼ ⓘ

Mirrored Ports (Ingress)

UP1 UP2 CONF POE1 POE2 POE3 POE4 ⓘ

☐ ☐ ☐ ☐ ☐ ☐ ☐

Mirrored Ports (Egress)

UP1 UP2 CONF POE1 POE2 POE3 POE4 ⓘ

☐ ☐ ☐ ☐ ☐ ☐ ☐

Configuration, Port Mirroring		
Global Status	Disabled	Kein Port-Mirroring
	Enabled	Port-Mirroring aktiv
Destination Port	Wählen Sie den Ziel-Port, an dem die Daten ausgegeben werden sollen.	
Mirrored Ports (Ingress)	Eingehender Datenverkehr des gewählten Ports wird gespiegelt.	
Mirrored Ports (Egress)	Ausgehender Datenverkehr des gewählten Ports wird gespiegelt.	

5.1.4.4 MAC Filter

Der MAC-Filter ist ein Zugangsschutz. Er gestattet nur Geräten mit bestimmter MAC-Adresse Zugang zum Netzwerk.

Bild 5-15 MAC Filter

MAC Filter Global Options

Port Security Status

Disabled  

Select Port

Port

UP1  

Configuration, MAC Filter		
Port Security Status	Disabled	Keine Port-Security
	Enabled	Port-Security für alle Ports aktiv
Port Security Mode	Stellen Sie ein, was passieren soll, wenn eine nicht erlaubte MAC-Adresse am gewählten Port erkannt wird.	
	None	Keine Security-Einstellungen
	Trap	Ein Trap wird an den SNMP-Trap-Server gesendet. Die Pakete werden nicht geblockt.
	Block	Ein Trap wird an den SNMP-Trap-Server gesendet. Die Pakete werden geblockt, bis eine erlaubte MAC-Adresse erkannt wird.  Zum Konfigurieren der SNMP-Traps siehe „SNMP“.
Last MAC Address Learnt	MAC-Adresse des zuletzt angeschlossenen Geräts	
Illegal Address Counter	Anzahl unerlaubter Zugriffe Jeder erstmalige Zugriff durch eine MAC-Adresse wird dabei gezählt. Erneute Zugriffe bereits bekannter MAC-Adressen werden gezählt, wenn in der Zwischenzeit eine andere MAC-Adresse zugegriffen hat.	
Clear Illegal Counter	Zähler zurücksetzen	
Allowed MAC Address	Erlaubte MAC-Adressen Pro Port können Sie bis zu 50 MAC-Adressen erlauben. Jede MAC-Adresse kann nur auf einem Port erlaubt werden. MAC-Adressen, die auf einem Port erlaubt sind, dürfen auch nicht dynamisch an anderen Ports gelernt werden. Somit ist ein Zugriff auf das Web-based Management oder das Netzwerk über eine an einem anderen Port erlaubte MAC-Adresse nicht möglich.	
Add new entry	Geben Sie eine neue erlaubte MAC-Adresse für den Port ein.	

5.1.4.5 PoE

Bild 5-16 PoE

Power Budget Alarm

PoE Power Threshold [%]

Please enter

90

PoE Port Configuration Table

Name	Port State	Port Mode	Power Pairs	Power Priority	Max Power Class
POE1	Enabled	Auto	Both	High	Class 8 or 5D (90 W)
POE2	Enabled	Auto	Both	High	Class 8 or 5D (90 W)
POE3	Enabled	Auto	Both	High	Class 8 or 5D (90 W)
POE4	Enabled	Auto	Signal	High	Class 4 or 3D (30 W)

Configuration, PoE

PoE Power Threshold

% des Leistungsbudgets

Wenn diese Schaltschwelle über- oder unterschritten wird, wird ein SNMP-Trap gesendet.

Zum Konfigurieren der SNMP-Traps siehe „SNMP“.

Configuration, PoE		
PoE Port Configuration Table	Name	Port
	Port State	Disabled: Keine PoE-Funktion auf dem Port Enabled: PoE-Funktion auf dem Port Scheduled: Entsprechend den Vorgaben aus dem Kalender, siehe „Time Profile Scheduling“ und „Time Profile Assignment“
	Port Mode	Auto: Automatische Erkennung von PoE-Geräten Force: Bei einigen PoE-Geräten ist die automatische Erkennung nicht möglich. Im Force-Modus ist die Spannung am Port immer verfügbar. ⓘ ACHTUNG: Gerätebeschädigung Wenn Sie Nicht-PoE-Geräte an einen Port im Force-Modus anschließen, werden diese Geräte beschädigt. – Aktivieren Sie den Force-Modus nur, wenn ein PoE-Gerät am Port angeschlossen ist.
	Power Pairs	Signal: PoE-Spannungsversorgung nur über Datenleitung 1, 2, 3, 6 (Signal-Pairs, auch: Alternative-A, Alt-A, Data, Endspan) Spare: PoE-Spannungsversorgung über Datenleitung 4, 5, 7, 8 (Spare Pairs, auch: Alternative-B, Alt-B, Midspan) Both: PoE-Spannungsversorgung über alle Aderpaare
	Power Priority	Wenn die verfügbare Gesamtleistung für die PoE-Geräte nicht mehr ausreicht, müssen einzelne Ports deaktiviert werden. Low: Geringste Priorität, der Port wird als Erster deaktiviert High: Mittlere Priorität Critical: Höchste Priorität Wenn mehrere Ports dieselbe Priorität haben, wird der Port mit der höheren Zahl zuerst nicht mehr versorgt. Beispiel: POE3 und POE4 haben die Priorität „Low“. POE4 wird zuerst abgeschaltet, POE3 wird weiterhin versorgt.
	Max. Power Class	Die PoE-Klasse bestimmt die maximale verfügbare Leistung am Port – Im Automodus: Klasse, die maximal zugewiesen werden kann – Im Force-Modus: maximal mögliche Leistungsabgabe. Wenn der Wert überschritten wird, wird der Port deaktiviert.
PoE Utilization Interval [s]	Intervall in Sekunden, in dem die Auslastung der PoE-Ports überwacht wird. Die Ergebnisse finden Sie unter „Diagnostics, PoE Utilization“.	
PoE Utilization Time Span	Dauer der Überwachung	

5.1.4.6 PoE Watchdog

Bild 5-17 PoE Watchdog

Select PoE Port	
Port	POE1  
PoE Watchdog	
Hold off [s]	Please enter 300 
Delay [s]	Please enter 10 

Configuration, PoE Watchdog		
Port	Wählen Sie den zu überwachenden Port.	
Hold off [s]	„Hold off“ beginnt, sobald das Powered Device mit Spannung versorgt wird. Nach Ablauf dieser Zeit wird der Watchdog scharfgeschaltet.	
Delay [s]	„Delay“ beginnt, sobald eine Watchdog-Bedingung zum ersten Mal auftritt. Nach Ablauf dieser Zeit wird die Watchdog-Aktion ausgelöst. Wenn die Watchdog-Bedingung innerhalb von „Delay“ zurückfällt, wird die Watchdog-Aktion nicht ausgelöst.	
Ping Watchdog Enable	Disabled	Watchdog sendet keine Pings
	Enabled	Der Watchdog sendet Pings an das Powered Device.
IP Address	IP-Adresse des Powered Device, das vom Watchdog überwacht werden soll	
Power Lower/Upper Limit Enable	Der Power-Watchdog überwacht die Leistungsaufnahme des Powered Device.	
Power Lower/Upper Limit Value [W]	Disabled	Keine Überwachung der Leistungsaufnahme
	Enabled	Wenn die untere/obere Schaltschwelle unterschritten bzw. überschritten wird, wird der Watchdog getriggert. Wählen Sie einen Wert zwischen 1 ... 100 W.
Bandwidth Lower/Upper Limit Enable	Der Bandbreiten-Watchdog überwacht die Kommunikation zwischen der Smart Ethernet Box und dem Powered Device. Unter „Diagnostics, Port Utilization“ finden Sie die aktuelle Bandbreite der Ports.	
Utilization Lower/Upper Limit Value [%]	Disabled	keine Überwachung der Bandbreite
	Enabled	Wenn die untere/obere Schaltschwelle unterschritten bzw. überschritten wird, wird der Watchdog getriggert. Wählen Sie einen Wert zwischen 0,01 ... 100 %.

5.1.4.7 Network Redundancy

RSTP ist ein Protokoll zum Deaktivieren von redundanten Pfaden in lokalen Netzwerken.

-  Allgemeine technische Informationen finden Sie unter „[RSTP - Rapid Spanning Tree Protocol](#)“.
-  Änderungen der Eigenschaften können dazu führen, dass der Rapid Spanning Tree komplett neu konfiguriert wird.

Bild 5-18 Network Redundancy

Spanning-Tree Configuration

RSTP Mode

802.1w

▼ ⓘ

Large Tree Support

Disabled

▼ ⓘ

Fast Ring Detection

Disabled

▼ ⓘ

Bridge Priority

Please enter
32768

ⓘ

Configuration, Network Redundancy		
RSTP Mode	Aktivieren Sie den RSTP-Modus auf allen Switches, die als RSTP-Komponenten im Netzwerk betrieben werden sollen.	
	Disabled	Kein RSTP
	802.1D-2004	RSTP aktiv
Large Tree Support	Proprietäre Funktion: nur möglich, wenn alle Geräte in der Struktur die Funktion unterstützen Durch die Funktion „Large Tree Support“ wird die maximal mögliche Anzahl Switches in einer RSTP-Topologie vergrößert, siehe A 2.8 „Large Tree Support“ .	
	Disabled	Kein Large Tree Support
	Enabled	Large Tree Support aktiv
Fast Ring Detection	Proprietäre Funktion: nur möglich, wenn alle Geräte in der Struktur die Funktion unterstützen Fast Ring Detection beschleunigt das Umschalten auf einen redundanten Pfad im Fehlerfall und ermöglicht die einfache Diagnose. Jedem Ring wird eine ID zugewiesen. Diese ID wird jedem Switch in dem jeweiligen Ring bekannt gemacht. Ein Switch kann gleichzeitig mehreren unterschiedlichen Ringen angehören. Umschaltzeit: 500 ms	
	Disabled	Kein Fast Ring Detection
	Enabled	Fast Ring Detection aktiv

Configuration, Network Redundancy		
Bridge Priority	Der Switch mit dem niedrigsten Wert ist die Root-Bridge. Wenn die Root-Bridge ausfällt, wird anhand der Bridge Priority die nächste Root-Bridge gewählt. Zulässig sind nur Vielfache von 4096. Der Wert wird automatisch auf das nächstgelegene Vielfache von 4096 gerundet. Wenn Sie auf „Apply“ klicken, wird der Initialisierungsmechanismus gestartet. Wert: 0 ... 61440 in Schritten von 4096	
Bridge Hello Time	Nur für Root-Bridge: Die Root-Bridge sendet ständig BPDUs im Abstand der Hello-Time. Wert: 1 ... 10 Sekunden, Werkseinstellung: 2 Sekunden	
Bridge Forward Delay	Nur für Root-Bridge: Zeitspanne, die der Switch benötigt, um vom Zustand „blocking“ zu „forwarding“ zu wechseln. Wert: 4 ... 30 Sekunden, Werkseinstellung: 15 Sekunden	
Bridge Max. Age	Nur für Root-Bridge: Der Parameter bestimmt, wie lange ein Port die RSTP-Information (BPDU) behält. Er wird von der Root-Bridge an alle Switches im Ring gesendet. So ist sichergestellt, dass jeder Switch im Netzwerk einen konstanten Wert hat, gegen den das Alter der gespeicherten Konfiguration getestet wird. Wert: 6 ... 40 Sekunden, Werkseinstellung: 20 Sekunden	
RSTP Port Configuration Table	Name	Port
	RSTP Enable	Disabled: Auf dem Port werden keine BPDUs gesendet oder empfangen Enabled: RSTP aktiviert, BPDUs werden gesendet und empfangen.
	Admin Path Cost	Sie können die Pfadkosten manuell eingeben. So können Sie z. B. einen Uplink bevorzugen. Wenn Sie die Werkseinstellung 0 beibehalten, werden die Pfadkosten anhand der Bandbreite automatisch ermittelt.
	Auto Edge	Disabled: Keine automatische Erkennung von Edge-Ports Enabled: Automatische Erkennung von Edge-Ports. An einem Edge-Port ist ein Endgerät angeschlossen, aber keine weiteren Switches oder Bridges. Der Port leitet keine BPDUs weiter.
	Admin Edge	Non-Edge: Der Port ist kein Edge-Port. Edge: Der Port ist ein Edge-Port.
	Priority	Priorität der Ports Der Port mit der mit dem höheren Wert hat die niedrigere Priorität. Wert: 0 ... 240 in Schritten von 16

5.1.4.8 SNMP

 Allgemeine technische Informationen finden Sie unter „SNMP - Simple Network Management Protocol“.

Bild 5-19 SNMP

SNMP

Note: For SNMPv2 the read community is public, the write community is admin user's password.

Note: For SNMPv3 the username is 'admin' and the password is the admin user's password, which has to be at least 8 characters long. The device's default password is too short!

Enable

SNMP v2

Trap Mode

Enable

Configuration, SNMP		
Mode	Disabled	Keine SNMP-Server-Funktion
	SNMP v2	Für den Lesezugriff benötigen Sie kein Passwort. Das Passwort für den Schreibzugriff ist das Administratorpasswort.
	SNMP v3	Der Benutzername ist admin, das Passwort ist das Administratorpasswort. Es muss mindestens acht Zeichen lang sein. Beachten Sie, dass das Standardpasswort zu kurz ist.
Trap Mode	Disabled	Keine SNMP-Traps
	Enabled	Senden von SNMP-Traps aktiviert
Trap Receiver List	Alle Trap-Server, die SNMP-Traps von diesem Gerät empfangen sollen	
Test Trap Connection	Testen Sie die Verbindung zum Trap-Server.	
Add New Trap Receiver	Fügen Sie einen Trap-Server hinzu, der SNMP-Traps empfangen soll.	
Trap List	Alle SNMP-Traps, die das Gerät versenden kann	
	Wählen Sie, bei welchen Aktionen SNMP-Traps versendet werden sollen.	

5.1.4.9 VLAN

Bild 5-20 VLAN

VLAN Configuration		
VLAN Mode Transparent Mode		
Configuration, VLAN		
VLAN Mode	Transparent Mode	Der Switch verarbeitet die eingehenden Datenpakete so wie unter A 1 „Frame-Switching“ beschrieben. Die Datenpakete werden weder in ihrer Struktur noch in ihrem Inhalt verändert. Die Information über die VLAN-Zugehörigkeit aus einem evtl. im Datenpaket enthaltenen Tag wird ignoriert.
	Active VLAN Mode	Der Switch leitet die Datenpakete anhand der VLAN-Zugehörigkeit weiter.
Nur sichtbar, wenn Sie „Active VLAN Mode“ gewählt haben:		
Management VLAN	VLAN, in dem das Web-based Management erreichbar sein soll	
VLAN Port Membership	VLAN ID	Liste der bisher angelegten VLAN
	VLAN Name	Wählen Sie, welcher Port sich im VLAN befinden soll:
	Ports	– -: Kein Mitglied im VLAN – U: Untagged Port – T: Tagged Port
	Delete VLAN	Gewähltes VLAN löschen. VLAN1 kann nicht gelöscht werden.
Add new VLAN	Um ein neues VLAN anzulegen, geben Sie die VLAN-ID und den Namen ein (maximal 31 Zeichen).	
VLAN Port Configuration Table	Name	Port
	VLAN ID	Wenn der empfangene Frame (das Paket) kein VLAN-Tag hat, wird der Frame diesem VLAN zugeordnet.
	Default Priority	Wenn der empfangene Frame (das Paket) kein VLAN-Tag hat, wird dem Frame diese Priorität gegeben.
	Filter	Disabled: – Der Port kann Frames in ein VLAN senden, auch wenn die VLAN-IDs von Port und VLAN voneinander abweichen. – Wenn der Port Frames empfängt, kann er diese auch an ein VLAN weiterleiten, das keine Frames an diesen Port sendet. Enabled: – Der Port sendet Frames nur in ein VLAN, wenn die VLAN-IDs von Port und VLAN übereinstimmen. – Wenn der Port Frames empfängt, kann er diese nur in ein VLAN mit übereinstimmender VLAN-ID weiterleiten, das auch Frames an diesen Port sendet.

5.1.4.10 LLDP

 Allgemeine technische Informationen finden Sie unter „[LLDP - Link Layer Discovery Protocol](#)“.

Bild 5-21 LLDP

LLDP

LLDP Mode

Enable

LLDP Transmit Interval (seconds)

Please enter
5

LLDP Reception

UP1UP2CONFPOE1POE2POE3POE4

☒☒☒☒☒☒☒

LLDP Transmission

UP1UP2CONFPOE1POE2POE3POE4

☒☒☒☒☒☒☒

Configuration, LLDP		
LLDP Mode	Disabled	Kein LLDP
	Enabled	LLDP aktiviert
	Send only	LLDP-BPDUs werden nur versendet
	Receive only	LLDP-BPDUs werden nur empfangen
LLDP Transmit Interval [s]	Intervall, in dem LLDP-Telegramme geschickt werden. Wert: 5 ... 32768 Sekunden	
LLDP Reception	Port nicht gewählt: Der Port ignoriert LLDP-Telegramme. ✓: Der Port wertet empfangene LLDP-Telegramme aus.	
LLDP Transmission	Port nicht gewählt: Der Port sendet keine LLDP-Telegramme. ✓: Der Port sendet LLDP-Telegramme im konfigurierten Intervall.	

5.1.4.11 AUX Power

Bild 5-22 AUX Power

AUX Power

Mode

Scheduled

▼ ⓘ

Configuration, AUX Power		
Mode	Der Schaltausgang (+/- AUX, 24 V DC) wird gesetzt:	
	Disabled	– 0 V
	Enabled	– Nach einem Neustart wird der Ausgang auf 24 V gesetzt. – Von der verfügbaren Leistung an den PoE-Ports werden 10 W abgezogen.
	Scheduled	– Entsprechend den Vorgaben aus dem Kalender, siehe „Time Profile Scheduling“ und „Time Profile Assignment“

5.1.4.12 Time Profile Scheduling

Hier können Sie bis zu zehn Zeitprofile für die PoE-Ports und den Schaltausgang definieren. In einem zweiten Schritt weisen Sie den Ports oder dem Ausgang das angelegte Zeitprofil zu, siehe [Kapitel „Time Profile Assignment“](#) auf Seite 69.

Bild 5-23 Time Profile Scheduling

Select Time Profile

Time Profile

Surveillance

Time Profile Name and Rhythm

Name

Please enter Surveillance

Rhythm

Weekly

Configuration, Time Profile Scheduling		
Time Profile	Wählen Sie ein Zeitprofil, das Sie konfigurieren möchten.	
Name	Vergeben Sie einen Namen für das Zeitprofil	
Rhythm	Wählen Sie einen täglichen oder wöchentlichen Rhythmus.	
Shortcuts and Help Functions	Set day all ON	An dem gewählten Tag ist der Port oder der Ausgang eingeschaltet.
	Set day all OFF	An dem gewählten Tag ist der Port oder der Ausgang ausgeschaltet.
	Copy day	Die Einstellungen des gewählten Tages werden für den Zieltag (Target Day) übernommen.
Time Profile Configuration Daily/Weekly	Setzen Sie einen Haken, wenn der Port oder der Ausgang in dem halbstündigen Zeit-Slot eingeschaltet sein soll, siehe Bild 5-24 .	

Bild 5-24 Time Profile Scheduling, Time Profile Configuration Weekly

Time Profile Configuration Weekly							
Timeframe	M	T	W	T	F	S	S
00:00 - 00:30	☒	☒	☒	☒	☒	☐	☐
00:30 - 01:00	☒	☒	☒	☒	☒	☐	☐
01:00 - 01:30	☒	☒	☒	☒	☒	☐	☐
01:30 - 02:00	☒	☒	☒	☒	☒	☒	☐
02:00 - 02:30	☒	☐	☒	☒	☒	☒	☐
02:30 - 03:00	☒	☐	☒	☒	☒	☒	☐

✓: Port oder Ausgang eingeschaltet.

5.1.4.13 Time Profile Assignment

Hier weisen Sie den PoE-Ports oder dem Schaltausgang ein Zeitprofil zu.

Bild 5-25 Time Profile Assignment

PoE

PoE Port

POE1

Port State

Enabled

Safe State

Disabled

Time Profile Assignment

☐ Surveillance

☐ Internet Hotspot

5.1.5 Diagnostics

5.1.5.1 Alarm & Events

Die Event-Tabelle speichert maximal 3000 Einträge. Danach werden die ältesten Einträge überschrieben. Bei einer großen Anzahl von Einträgen kann das Öffnen der Event-Tabelle einige Sekunden dauern.

In der Werkseinstellung ist das dauerhafte Speichern **deaktiviert**. Bei einem Neustart werden die Ereignisse gelöscht.

Diagnostics, Alarm & Events		
System Uptime	Zeit seit dem letzten Boot-Vorgang	
Current System Time	Aktuelle Systemzeit in UTC	
Event Count	Anzahl der Ereignisse	
Event Table as CSV File	Export der Ereignistabelle als CSV-Datei	
Clear Event Table	Löschen aller bisherigen Einträge	
Persistent Event Logging	Disabled	ⓘ ACHTUNG: Bei einem Neustart werden die Ereignisse gelöscht.
	Enabled	Ereignisse werden dauerhaft gespeichert Häufiges dauerhaftes Speichern kann die Lebenszeit des internen Speichers verkürzen.

5.1.5.2 Local Diagnostics

Hier sehen Sie den Zustand folgender Komponenten:

- PoE-Ports
- Ethernet-Ports
- Schaltausgang (+/- AUX, 24 V DC)
- Tür, offen/geschlossen
- Überspannungsschutzmodule

5.1.5.3 Port Table

Unter „Physical Ports“ sehen Sie den Verbindungsstatus aller Ports.

Unter „Dot1x Port Configuration“ sehen Sie den Authentifizierungsstatus der Ports sowie Anzahl und Quelle der empfangenen EAPOL-Frames.

EAPOL (Extensible Authentication Protocol over Local Area Networks) ist ein Nachrichtenformat zum Austausch von Authentifizierungsinformationen zwischen dem Supplikanten und dem Authenticator.

5.1.5.4 Port Counter

Alle Zahlen beziehen sich auf die Zeit seit dem letzten Reboot oder dem letzten Zurücksetzen der Zählerstände.

Unter „Port Counter Overview“ finden Sie :

- Anzahl der empfangenen Pakete
- Anzahl der gesendeten Pakete
- Anzahl der CRC-Fehler
- Anzahl der Kollisionen

Unter „Transmission Details“ finden Sie:

- Anzahl der übertragenen Unicast-, Multicast- und Broadcast-Pakete
- Anzahl der Kollisionen

Unter „Receiving Details“ finden Sie:

- Anzahl der empfangenen Unicast-, Multicast- und Broadcast-Pakete
- Anzahl der CRC-Fehler
- Anzahl der Oversize-Pakete (>1518 Bytes)
- Anzahl der Undersize-Pakete (<64 Bytes)

Mit „Clear“ löschen Sie die aufgezeichneten Daten.

5.1.5.5 Port Counter Details

Unter „Port Counter Details“ sehen Sie die Auslastung der einzelnen Ports in Prozent. Sie finden eine detaillierte Aufstellung aller empfangenen und gesendeten Pakete nach Übertragungsart und Größe sowie die Anzahl fehlerhafter Pakete.

Mit „Clear“ setzen Sie die komplette Statistik auf „0“ zurück.

5.1.5.6 Port Utilization

Hier sehen Sie die Auslastung der Ports in Form von Diagrammen.

5.1.5.7 MAC Address Table

Auf dieser Seite finden Sie eine Liste der aktuellen Teilnehmer im Netzwerk. Sie können die Auflistung im CSV-Format herunterladen.

Mit „Clear“ löschen Sie die aufgezeichneten Daten.

5.1.5.8 PoE Table

Hier finden Sie:

- Verfügbare PoE-Leistung, gesamt
- Aktuelle Leistungsaufnahme der PoE-Geräte, gesamt
- Zugewiesenes Leistungsbudget, gesamt
- Noch verfügbare PoE-Leistung

Die Tabelle „Port Overview“ zeigt:

- Status von Signal-Pair und Spare Pair
- Zugewiesene PoE-Klasse von Signal-Pair und Spare Pair
- Leistungsabgabe von Signal-Pair und Spare Pair
- Leistungsabgabe, gesamt

5.1.5.9 PoE Utilization

Hier sehen Sie die Auslastung der PoE-Ports in Form von Diagrammen. Das ermöglicht eine grafische Diagnose der Budgetverteilung und -historie.

Die PoE-Überwachung konfigurieren Sie unter „Configuration, PoE“, siehe [Kapitel „PoE“ auf Seite 58](#).

5.1.5.10 Network Redundancy

Hier finden Sie alle Informationen zum RSTP-Status und den virtuellen Ports.

5.1.5.11 LLDP Topology

Hier finden Sie Informationen zu den benachbarten Ports und angeschlossenen Geräten.

5.1.5.12 Snapshot

Hier erstellen Sie einen Snapshot der aktuellen Geräteparameter. So können Sie Konfiguration und Status eines Geräts sichern.

Die Datei „snapshot.tar.gz“ laden Sie auf Ihren Rechner herunter.

5.2 Mode-Taster

Mit dem Mode-Taster können Sie die Betriebsart des Geräts umstellen, auch wenn Sie keinen Zugriff auf eines der Management-Interfaces haben.

Über den Taster rufen Sie den Smart Mode auf und wählen die gewünschte Funktion. Die jeweils aktive Funktion wird durch das Blinken von sechs LEDs angezeigt.

Mögliche Funktionen:

- Rücksetzen auf Werkseinstellungen
- Statische IP-Adresse einstellen, andere Einstellungen bleiben unverändert
192.168.0.254, Netzmaske 255.255.255.0
- Rücksetzen auf DHCP (Standard-IP-Konfiguration), andere Einstellungen bleiben unverändert
- BootP einstellen, siehe 5.2.1
- Unmanaged Mode einstellen, siehe 5.2.2
- Rücksetzen auf eine vorherige Firmware-Version, wird nicht im Smart Mode gewählt, siehe 5.2.3

Smart Mode aufrufen

Den Smart Mode können Sie **nur unmittelbar nach dem Boot-Vorgang** aufrufen, sobald alle LEDs erloschen sind.

- Halten Sie den Taster mindestens fünf Sekunden lang gedrückt. Wenn alle LEDs dauerhaft grün leuchten, lassen Sie den Taster los.
- ↪ Sie sind jetzt im Smart Mode. Alle LEDs blinken in regelmäßigen Abständen. Die Funktion „Verlassen ohne Änderung“ ist gewählt.
- Um eine andere Funktion zu wählen, drücken Sie den Taster mehrmals kurz.
 - ○ = Aus
 - ● = Ein

Tabelle 5-2 LEDs im Smart Mode

Funktion	CONF		UP 2		UP 1	
Verlassen ohne Änderung	○	○	○	○	○	●
Rücksetzen auf Werkseinstellungen	○	○	○	○	●	●
Statische IP-Adresse (192.168.0.254)	○	○	○	●	●	●
DHCP (Standard-IP-Konfiguration)	○	○	●	●	●	●
BootP	○	●	●	●	●	●
Unmanaged Mode	●	●	●	●	●	●

Einstellung übernehmen

- Halten Sie den Taster mindestens fünf Sekunden lang gedrückt. Wenn alle LEDs dauerhaft leuchten, lassen Sie den Taster los.
- ↪ Die zuletzt gewählte Funktion ist jetzt gespeichert und aktiviert. Wenn Sie „Rücksetzen auf Werkseinstellungen“ oder „DHCP“ gewählt haben, wird der Switch neu gestartet.

5.2.1 BootP

Für die IP-Adressvergabe nutzt das Gerät das BootP-Protokoll. Das Internet stellt eine Vielzahl von BootP-Servern zur Verfügung. Sie können ein beliebiges Programm für die Adressvergabe nutzen.



Außerdem benötigen Sie das „BootP IP-Adressierungstool“. Dieses Tool können Sie kostenfrei herunterladen im Download-Bereich unter phoenixcontact.com/product/1102626.

Bei der ersten Inbetriebnahme sendet das Gerät ununterbrochen BootP-Requests, bis es eine gültige IP-Adresse erhält. Wenn es eine IP-Adresse erhalten hat, sendet das Gerät keine weiteren BootP-Requests.

5.2.2 Unmanaged Mode

Im Unmanaged Mode können Sie den Switch ohne IP-Adresse nutzen. Dabei nimmt der Switch die statische IP-Adresse 0.0.0.0 an. Subnetzmaske und Gateway werden ebenfalls auf 0.0.0.0 konfiguriert. Dadurch lässt sich das Web-based Management nicht mehr erreichen. Der Switch sendet keine BootP- und DHCP-Requests mehr.

Die Redundanzmechanismen zur Schleifenunterdrückung (RSTP, FRD, LTS) bleiben im Unmanaged Mode aktiv.

- Sie müssen diese Redundanzmechanismen im Managed Mode konfigurieren. Beim Umschalten auf den Unmanaged Mode bleiben sie aktiv.

Unmanaged Mode verlassen

- Wählen Sie im Smart Mode eine andere Funktion.

Oder:

- Setzen Sie das Gerät auf Werkseinstellungen zurück.

5.2.3 Rücksetzen auf eine vorherige Firmware-Version



ACHTUNG: Fehlfunktion

Das Gerät muss einmal ein Firmware-Update durchlaufen haben, bevor Sie diese Funktion nutzen können.

Sie können das Gerät auf eine vorherige Firmware-Version rücksetzen, falls z. B. ein Firmware-Update fehlgeschlagen ist.

- Trennen Sie das Gerät von der Versorgungsspannung.
- Halten Sie den Mode-Taster gedrückt, während Sie das Gerät wieder einschalten.
- Die LEDs blinken grün. Lassen Sie den Mode-Taster nach einer Sekunde wieder los.
- ↪ Die LEDs blinken, danach startet das Gerät neu.
- ↪ Das Gerät wurde jetzt auf das zweite Firmware-Image umgeschaltet.
- Prüfen Sie im Web-based Management unter „Information, Device Status“, welche Firmware-Version aktiv ist.

Falls erforderlich, können Sie auf dieselbe Weise wieder auf das erste Firmware-Image umschalten.

5.3 Verhalten bei Neustart und im Fehlerfall

Äußere Einflüsse, wie z. B. große Überspannungseignisse, können die Abläufe der internen Prozessoren in der Smart Ethernet Box stören. Der interne Überwachungsprozess erkennt solche Störungen und löst ggf. einen Neustart aus. Ein ähnliches Verhalten kann auftreten, wenn durch Änderungen der Gerätekonfiguration ein Neustart erforderlich ist.

Im Folgenden wird das Verhalten bei einem erforderlichen Neustart beschrieben, der über das Web-based Management herbeigeführt wurde.

Ausgangsverhalten der Ports

- PoE-Ports: PoE-Versorgungsspannung, Datenverbindung
- Konfigurations-Port: Datenverbindung
- Uplink-Ports: Datenverbindung
- Schaltausgang (+/- AUX): Versorgungsspannung

Während des Neustarts sind alle Ports deaktiviert.

Nach dem Neustart sind die Ports aktiviert oder deaktiviert je nach gespeicherter Konfiguration. Deaktivierte Ports bleiben deaktiviert.

6 Gerätetausch, Gerätedefekt und Reparatur

6.1 Gerätetausch



WARNUNG: Gefährliche Berührungsspannung

Demontieren Sie die Smart Ethernet Box nur im spannungsfreien Zustand.



WARNUNG: Absturzgefahr

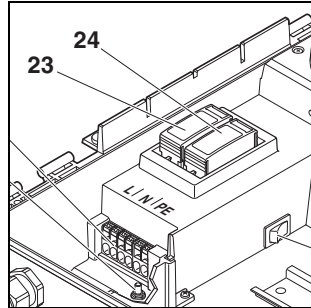
- Demontieren Sie die Smart Ethernet Box ggf. mit zwei Personen.
- Wenn Sie Steig- und Montagehilfen verwenden, z. B. Leitern oder Arbeitsbühnen, beachten Sie die einschlägigen Sicherheitsvorschriften.
- Achten Sie immer auf einen sicheren Stand.

Sie können die Smart Ethernet Box bei Bedarf austauschen.

- Demontieren Sie die Smart Ethernet Box wie unter „[Demontieren](#)“ auf [Seite 29](#) beschrieben.
- Tauschen Sie die Smart Ethernet Box gegen eine identische Smart Ethernet Box (gleiche Artikelnummer) aus.

6.1.1 Überspannungsschutz austauschen

Bild 6-1 Module für Überspannungsschutz



Die Smart Ethernet Box enthält zwei steckbare Module für den Überspannungsschutz der Netzspannung.

Tabelle 6-1 Module für Überspannungsschutz

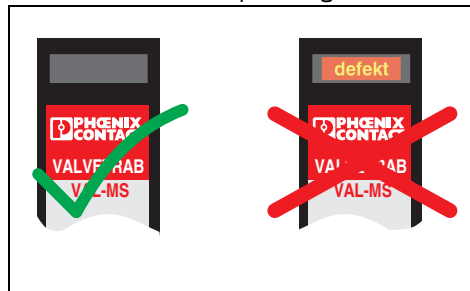
	Smart Ethernet Box mit UL-Zulassung	Smart Ethernet Box ohne UL-Zulassung
Variante Überspannungsschutz bei Auslieferung:	Heavy-Duty-Variante	Basisvariante
Pos. 23, L-N	VAL-MS 320 HD ST, 1224886	VAL-MS 230 ST, 2798844
Pos. 24, N-PE	F-MS 12 HD ST, 1224885	VAL-MS 350 VF ST, 2856595

i Verwenden Sie entweder Module der Heavy-Duty-Variante **oder** der Basisvariante. Verwenden Sie **nicht** verschiedene Varianten in einem Gerät. Wir empfehlen die Verwendung der Heavy-Duty-Variante in allen Geräten.

Wenn die rote Anzeige "defekt" erscheint, ist das Modul beschädigt. Alternativ können Sie eine Alarmmeldung über das Web-based Management oder SNMP konfigurieren.

- Tauschen Sie das Modul gegen ein Modul gleichen Typs aus (siehe [Tabelle 6-1](#))
- Beachten Sie die Packungsbeilage des Moduls.

Bild 6-2 Überspannungsschutzmodule



6.2 Gerätedefekt und Reparatur

Reparieren Sie die Smart Ethernet Box oder die enthaltenen Komponenten nicht selbst. Reparaturen darf nur der Hersteller vornehmen. Der Hersteller haftet nicht für Schäden aus Zuwiderhandlung.

- 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 „[Umgebungsbedingungen](#)“ auf Seite 87).
 - 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 Wartung und Entsorgung

7.1 Wartung



WARNUNG: Gefährliche Berührungsspannung

- Die Wartung ist von elektrotechnisch qualifiziertem Fachpersonal durchzuführen.
- Trennen Sie die Smart Ethernet Box bei Wartungsarbeiten von allen Energiequellen.
- Beachten Sie die Hinweise unter „Sicherheitshinweise“ auf Seite 7 und „Elektrischer Anschluss“ auf Seite 30.

Wartungsintervall und Dokumentation

- Prüfen Sie die Smart Ethernet Box in regelmäßigen Abständen, mindestens jedoch einmal jährlich. Das Wartungsintervall hängt auch von den Einsatz- und Umgebungsbedingungen ab. Bauteile und Komponenten, die häufiger Benutzung oder Beanspruchung unterliegen, müssen in entsprechend kürzeren Intervallen geprüft werden.
- Dokumentieren Sie die durchgeführten Wartungsschritte.

Sauberkeit

- Achten Sie bei der Wartung darauf, dass Staub und Feuchtigkeit **nicht** in das Innere der Smart Ethernet Box gelangen.

Bei Mängeln und Defekten

- Sobald Sie Mängel oder Defekte an der Smart Ethernet Box feststellen, müssen diese unverzüglich behoben werden. Wenn eine unmittelbare Gefahr durch eine mangelhafte elektrische Anlage besteht, darf diese nicht weiter betrieben werden.
- Setzen Sie die Smart Ethernet Box bei Gefahr von Personen- und Sachschäden sofort außer Betrieb. Vor der Wiederinbetriebnahme muss die Smart Ethernet Box unbedingt wieder in den ordnungsgemäßen Zustand versetzt werden.

Räumliche Grenzen, sichere Montage und Einsatzort

- Prüfen Sie die räumlichen Grenzen am Einsatzort (Empfehlung: B = 1000 mm, H = 2000 mm, T = 1000 mm). Die geforderten räumlichen Grenzen für Betrieb und Instandhaltung sind für eine sichere Anwendung einzuhalten und ggf. wiederherzustellen.
- Kontrollieren Sie den festen Sitz der Smart Ethernet Box am Einsatzort (z. B. Verschraubung).
- Stellen Sie sicher, dass die Smart Ethernet Box für die Bedingungen am Einsatzort ausgelegt ist.

Gehäuse und Dichtungen

- Prüfen Sie das Gehäuse auf sichtbare Beschädigungen und ggf. Korrosion.
- Reinigen Sie die äußeren Oberflächen des Gehäuses mit einem feuchten Reinigungstuch. Entfernen Sie grobe Verschmutzungen mit einer weichen Bürste. Damit die Oberfläche nicht beschädigt wird, verwenden Sie keine aggressiven oder ätzenden Reinigungsmittel, keine Verdünnung, keine Scheuermittel und keine harten Gegenstände.
- Prüfen Sie das Öffnen und Schließen der Gehäusetür. Behandeln Sie die Scharniere ggf. mit Schmiermittel.
- Prüfen Sie die ordnungsgemäße Verriegelung der Gehäusetür.
- Prüfen Sie die Dichtigkeit des Gehäuses. Stellen Sie sicher, dass sich kein Kondenswasser im Innenraum befindet.

Verkabelung und Komponenten

- Prüfen Sie alle Dichtungen auf Verformungen, Risse und Verschmutzung. Alle Dichtungen müssen regelmäßig gewartet werden, um die Schutzart des Gehäuses zu gewährleisten.
- Pflegen Sie alle Dichtungen mit einem geeigneten Pflegemittel.
- Kontrollieren Sie regelmäßig alle Komponenten, Kabel, Klemmpunkte, Leiterverbindungen und Kennzeichnungen.
- Prüfen Sie die Zugentlastung der Kabel.
- Prüfen Sie den festen Sitz und die Dichtigkeit aller Kabelverschraubungen und Steckverbindungen.
- Kontrollieren Sie die Kabelführung und die Biegeradien. Um Beschädigungen der Kabel zu vermeiden, stellen Sie sicher, dass die Kabel nicht zu stark geknickt sind.
- Prüfen Sie die Kabel, Kabelverbindungen und Komponenten auf Anzeichen von Überhitzung, wie z. B. Verfärbung oder Verformung. Wenden Sie sich bei Auffälligkeiten an Ihre jeweilige Ländervertretung, um das weitere Vorgehen abzustimmen. Die Adresse erfahren Sie unter phoenixcontact.com. Der Auslöser der Überhitzung muss vor der Wiederinbetriebnahme unbedingt identifiziert und in einen ordnungsgemäßen Zustand versetzt werden.
- Prüfen Sie die Drehmomente aller Verbindungen (siehe Kapitel 8.2). Ziehen Sie lose Verbindungen unter Berücksichtigung des Drehmoments fest.
- Prüfen Sie alle Steckverbindungen auf festen Sitz und ordnungsgemäße Funktion.

Schutzleiter

- Prüfen Sie alle Verbindungen des Schutzleitersystems, wie z. B. Leiter, Erdungsschrauben, Erdungsbolzen oder Erdungsschienen.
- Stellen Sie sicher, dass alle Verbindungen noch zuverlässig angeschlossen sind.

Isolationsmessung

- Ziehen Sie vor der Isolationsmessung alle Stecker und Überspannungsschutzmodule, um ein korrektes Messergebnis zu erhalten. Setzen Sie die Stecker nach der Isolationsmessung wieder ein.

7.2 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 phoenixcontact.com.

- Löschen Sie vor der Rückführung personenbezogene Daten.
- Entsorgen Sie nicht mehr benötigte Verpackungsmaterialien (Kartonage, Papier, Luftpolsterfolie etc.) im Hausmüll gemäß den jeweils gültigen nationalen Vorschriften.

8 Technische Daten

8.1 Bestelldaten

Beschreibung	Typ	Art.-Nr.	VPE
Smart Ethernet Box zum Anschließen von PoE-Endgeräten, Managed Switch, Überspannungsschutz integriert, Versorgungsspannung 100 ... 240 V AC, Wand- oder Mastmontage			
4 PoE-Ports, 2 Uplink-Ports (SFP-Slots)	SCX 4POE 2LX	1102626	1
2 PoE-Ports, 2 Uplink-Ports (SFP-Slots)	SCX 2POE 2LX	1108543	1
4 PoE-Ports, 2 Uplink-Ports (RJ45)	SCX 4POE 2T	1108542	1
2 PoE-Ports, 2 Uplink-Ports (RJ45)	SCX 2POE 2T	1108544	1

8.1.1 Zubehör

Überspannungsschutz, siehe Tabelle 6-1	Typ	Art.-Nr.	VPE
Ersatzstecker für die Smart Ethernet Box SCX für die Strecke N-PE	F-MS 12 HD ST	1224885	10
Ersatzstecker für die Smart Ethernet Box SCX für die Strecke L-N	VAL-MS 320 HD ST	1224886	10
Überspannungsschutzstecker Typ 2 mit Hochleistungsvaristor für VAL-MS-Basiselement, thermisch überwacht, optische Defektmeldung, Ausführung: 230 V AC	VAL-MS 230 ST	2798844	10
Überspannungsschutzstecker Typ 2 mit Reihenschaltung aus Hochleistungsvaristor und Funkenstrecke für VAL-MS-Basiselement, leckstromfrei	VAL-MS 350 VF ST	2856595	10
Überspannungsschutz gem. Class E _A (CAT6 _A), für Gigabit-Ethernet (bis 10 GBit/s), Token-Ring, FDDI/CDDI, ISDN, DS1. Geeignet für Power-over-Ethernet (PoE++ / 4PPoE) "Mode A" und "Mode B". RJ45-Zwischenstecker mit separater Erdungsleitung und Erdanschluss-Rastfuß für Tragschienen NS 35	DT-LAN-CAT.6+	2881007	1

Montagematerial	Typ	Art.-Nr.	VPE
Mastschellen, 2 Stück, mit Schnellmontageanschluss zur Installation an Masten mit einem Durchmesser von 51 ... 127 mm	SCX-CLAMP 14X51-127	1175556	1
Mastschellen, 2 Stück, mit Schnellmontageanschluss zur Installation an Masten mit einem Durchmesser von 102 ... 254 mm	SCX-CLAMP 14X102-254	1188634	1
Stabiler Türriegel mit Verriegelungslasche zum sicheren Verschießen der Smart Ethernet Box, schützt vor unbefugtem Zugriff, für ein Vorhängeschloss mit einem Bügeldurchmesser bis zu 12 mm	SCX-DOOR-LOCK	1184401	1

SCX xPOE...

Montagematerial [...]	Typ	Art.-Nr.	VPE
Der FL TRAGSCHIENENADAPTER 22.5 wurde konzipiert, um 22,5 mm breite Produkte in beliebiger Ausrichtung bündig auf einer standardmäßigen 35-mm-Tragschiene montieren zu können.	FL DIN-RAIL ADAPTER 22.5	1085485	1
Der FL TRAGSCHIENENADAPTER 40 wurde konzipiert, um 40 mm breite Produkte in beliebiger Ausrichtung bündig auf einer standardmäßigen 35-mm-Tragschiene montieren zu können.	FL DIN-RAIL ADAPTER 40	1085484	1
Spleißbox mit 12 Nuten für 12 Adern	FOC-SPLICEHOLDER:10	1086804	10
Schrumpfspleißschutz, Bauform: gerade, Schutzart: IP20, Kabelabgang: oben und unten, Farbe: transparent	FOC-SHRINKSPLICE-PROTECT	1019676	12
Crimpspleißschutz, Bauform: gerade, Schutzart: IP20, Anschlussart: Crimp, Kabelabgang: oben und unten, Farbe: metallisch blank	FOC-CRIMPSPLICE-PROTECT	1019678	12
Kabel	Typ	Art.-Nr.	VPE
Netzwerkkabel, Schutzart: IP20, Polzahl: 8, 1 GBit/s, CAT5, Kabelabgang: gerade, Ethernet	NBC-R4AC-R4AC-IE8/.../...	1411842	1
LWL-Leitung, Kabellänge: 5 m, OM4 OM4-Duplex-Jumper, Multimode, LC-LC, UPC-Schliff	FOC-LC:PA-LC:PA-OM4:D01/5	1115621	1
LWL-Leitung, Kabellänge: 5 m, OS2 OS2-Duplex-Jumper, Singlemode, LC-LC, UPC-Schliff	FOC-LC:PA-LC:PA-OS2:D01/5	1115626	1
Software	Typ	Art.-Nr.	VPE
FL Network Manager, SNMP-basierte Konfigurations- und Firmware-Update-Software, zur einfachen Inbetriebnahme von Managed Switches	FL NETWORK MANAGER BASIC	2702889	1
SFP-Module für SCX 4POE 2LX und SCX 2POE 2LX	Typ	Art.-Nr.	VPE
Gigabit-SFP-WDM-Modul für Übertragung bis maximal 10 km auf einer Faser mit einer Wellenlänge von 1550/1310 nm	FL SFP WDM10-B	2702441	1
Gigabit-SFP-Modul für Übertragung bis zu 2 km mit einer Wellenlänge von 1310 nm	FL SFP SX2	2702397	1
Gigabit-SFP-WDM-Modul für Übertragung bis maximal 10 km auf einer Faser mit einer Wellenlänge von 1310/1550 nm	FL SFP WDM10-A	2702440	1
Gigabit-SFP-Modul für Übertragung bis zu 10 km mit einer Wellenlänge von 1310 nm	FL SFP LX10-B	1025401	1
Gigabit SFP-Modul für Übertragung bis zu 100 m	FL SFP GT	2989420	1
Für Montage nach UL	Typ	Art.-Nr.	VPE
NPT-Adapter, Edelstahl, M20 auf 1/2"	SCX M20-1/2NPT	1247389	1

8.2 Technische Daten

Versorgung		
Versorgungsspannungsbereich		100 V AC ... 240 V AC (einphasig)
Toleranz		-15 % ... +10 %
Nennfrequenz		50 Hz ... 60 Hz
Nennstrombereich		1,2 A ... 2,9 A
Leistungsschutzschalter/Sicherung		Leistungsschutzschalter, 6 A ... 16 A, Charakteristik B, C, D, K
Bemessungsisolationsspannung		3 kV AC (Eingang / Ausgang, IEC/EN 60950-1)
Schutzklasse		I (Schutzerdung aller leitenden Gehäuseteile)
Stromversorgungssystem		TN, TT
Anschlussart		
Push-in-Federanschluss		
Abisolierlänge		10 mm
Leiterquerschnitt		
	flexibel	0,20 mm ² ... 6,00 mm ²
	starr	1,00 mm ² ... 6,00 mm ²
	AWG flexibel	24 AWG ... 10 AWG
	flexibel mit Aderendhülse ohne Kunststoffhülse	0,2 mm ² ... 4 mm ²
	flexibel mit Aderendhülse mit Kunststoffhülse	0,2 mm ² ... 4 mm ²
	2 Leiter gleichen Querschnitts flexibel mit TWIN-Aderendhülse mit Kunststoffhülse	0,5 mm ² ... 1,5 mm ²
Kabelverschraubung		
Gewindeart Kabelverschraubung		5x M20, 5x M25 nach UL: 2x M20, 5x M25
Anzugsdrehmoment Kabelverschraubung		
	M20	2 Nm
	M20, UL	4 Nm
	M25	3,5 Nm
	M25, UL	5 Nm
Leitungsaußendurchmesser		
	M20	6 mm ... 12 mm
	M25	6 mm ... 10 mm
Zugentlastung		IEC 62444



Für Montage nach UL verwenden Sie Conduit-Fittings: 3x 1/2" NPT (L, N, PE), siehe [Seite 82](#)

SCX xPOE...

PoE-Ports	SCX 4POE...	SCX 2POE...
Anzahl der Ports	4	2
Benennung	Ethernet / Fast Ethernet / Gigabit-Ethernet	
Anschlussart	RJ45-Buchse	
Hinweis zur Anschlussart	Autonegotiation und Autocrossing	
Übertragungsmedium	Kupfer	
Übertragungsgeschwindigkeit	10/100/1000 MBit/s	
Übertragungslänge	100 m (pro Segment)	
Power-over-Ethernet	PoE-Standard IEEE 802.3bt, at, af	PoE-Standard IEEE 802.3bt, at, af
Ausgangsleistung maximal	165 W (>55 °C Derating)	165 W (>55 °C Derating)
	155 W (wenn Schaltausgang aktiv, >55 °C Derating)	155 W (wenn Schaltausgang aktiv, >55 °C Derating)
	90 W (pro Port POE1...3, >50 °C Derating)	90 W (pro Port POE1/2, >50 °C Derating)
	30 W (POE4)	-
Uplink-Ports	SCX...2LX	SCX...2T
Anzahl der Ports	2	2
Anschlussart	SFP-Ports	RJ45-Buchse
Hinweis zur Anschlussart	SFP-Module als Zubehör erhältlich	-
Übertragungsmedium	je nach verwendetem SFP-Modul	Kupfer
Übertragungsgeschwindigkeit	100/1000 MBit/s (je nach verwendetem SFP-Modul)	10/100/1000 MBit/s
Übertragungslänge	<80 km (je nach verwendetem SFP-Modul)	100 m (pro Segment)
Konfiguration		
Anzahl der Ports	1	
Anschlussart	RJ45	

Store and Forward Switch, normkonform nach IEEE 802.3

Management	Web-based Management (HTTP/HTTPS) SNMPv2/v3 Command Line Interface (Telnet, SSH)
Diagnosefunktionen	RMON History LLDP (Link Layer Discovery Protocol) SNMP-Traps N:1-Port-Mirroring ACD (Address Conflict Detection)
Filterfunktionen	Port-Priorisierung VLAN (bis zu 32 VLANs)
Redundanz	RSTP (Rapid Spanning Tree Protocol nach IEEE 802.1D-2004) Large Tree Support FRD (Fast Ring Detection)
Zeitsynchronisierung	SNTP (Simple Network Time Protocol)
IP-Parametrierung	DHCP-Client BootP Statische IP-Adresse
Weitere Funktionen	Jumbo Frames
MAC-Adresstabelle	8k

Schaltausgang

Anzahl der Ports	1
Konfiguration	Konfiguration über Web-based Management
Ausgangsnnennspannung	24 V DC $\pm 10\%$ (Versorgung für Geräte innerhalb der Smart Ethernet Box)
Ausgangsstrom	300 mA (typisch)
Bürde/Ausgangslast Stromausgang	keine induktive Last
Anschlussart	Push-in-Federanschluss
Abisolierlänge	10 mm
Leiterquerschnitt	

flexibel 0,2 mm² ... 1,5 mm²starr 0,2 mm² ... 1,5 mm²

AWG 24 AWG ... 16 AWG

flexibel mit Aderendhülse ohne Kunststoffhülse 0,25 mm² ... 1,5 mm² (Abisolierlänge 8 mm)flexibel mit Aderendhülse mit Kunststoffhülse 0,25 mm² ... 0,75 mm² (Abisolierlänge 8 mm)Für Montage nach UL verwenden Sie Conduit-Fittings: 3x 1/2" NPT (L, N, PE), siehe [Seite 82](#)**Überspannungsschutz**

IEC-Prüfklasse	II T2
Normen/Bestimmungen	IEC 61643-11, EN 61643-11

Allgemeine Daten				
Abmessungen (B/H/T)	284 mm x 364 mm x 121 mm			
Material				
Gehäuse	Polycarbonat PC			
Kabelverschraubung	Polyamid			
Dichtung der Kabelverschraubung, schwarz	Neopren			
Farbe	lichtgrau 7035			
Schutzart	IP65 (nach DIN EN 60529: vollständiger Berührungsschutz, Staub kann nicht eindringen, Strahlwasserschutz aus beliebiger Richtung)			
Schlagfestigkeit	IK10 (nach IEC 62262: Schlagenergie 20 J, entspricht 5 kg aus 40 cm Höhe)			
Verschmutzungsgrad	2			
Brennbarkeitsklasse nach UL 94				
Gehäuse	V0 (Verlöschen einer vertikal eingespannten Probe innerhalb von 10 Sekunden, kein brennendes Abtropfen von Kunststoffschmelze, maximal 60 Sekunden Nachglimmen)			
Kabelverschraubung	V2 (Verlöschen einer vertikal eingespannten Probe innerhalb von 30 Sekunden, brennendes Abtropfen ist zulässig)			
Brandschutz	DIN EN 45545-2, Anforderungssatz R22, Gefährdungsstufe HL3			
Vibrationsfestigkeit nach EN 60068-2-6/IEC 60068-2-6	1g			
Schock nach EN 60068-2-27/IEC 60068-2-27	15g, 11 ms			
Halogenfreiheit	IEC 61249-2-21 (Gehäuse, Brom: < 900 ppm, Chlor: < 900 ppm, Gesamthalogenanteil: < 1500 ppm)			
Sonstige Beständigkeit	UV-beständig nach UL746C, f1-Listung/Bewertung (Outdoor-Gehäuse, 1000 Stunden unter Xenon-Bewitterung, 7-tägige Wassertauchprüfung)			
 Gehäuse (UL50/50E): UL (NEMA) Gehäuseklassifizierung: 4X, wasserdicht und korrosionsbeständig, geeignet für den Innen- und Außenbereich				
Überspannungskategorie				
Bei gesteckten Schutzmodulen	III			
Ohne Schutzmodule	II			
MTTF (mittlere Dauer bis zum Ausfall), SN 29500 Standard	SCX 4POE 2LX	SCX 2POE 2LX	SCX 4POE 2T	SCX 2POE 2T
Temperatur 25 °C, Arbeitszyklus 21 % (5 Tage pro Woche, 8 Std. pro Tag)	450 Jahre	547 Jahre	441 Jahre	496 Jahre
Temperatur 40 °C, Arbeitszyklus 34,25 % (5 Tage pro Woche, 12 Std. pro Tag)	228 Jahre	272 Jahre	224 Jahre	247 Jahre
Temperatur 40 °C, Arbeitszyklus 100 % (7 Tage pro Woche, 24 Std. pro Tag)	96 Jahre	113 Jahre	92 Jahre	105 Jahre

Umgebungsbedingungen

Umgebungstemperatur

Betrieb -40 °C ... 70 °C (>50 °C Derating)

Lagerung/Transport -40 °C ... 85 °C

Zulässige Luftfeuchtigkeit

Betrieb 10 % ... 95 % (keine Betauung)

Höhenlage

2000 m

Derating

Bild 8-1 Derating (PoE-Leistung gesamt)

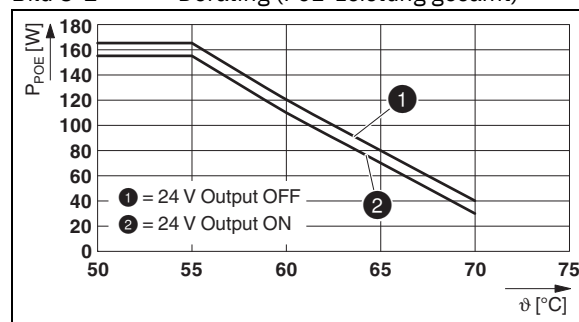
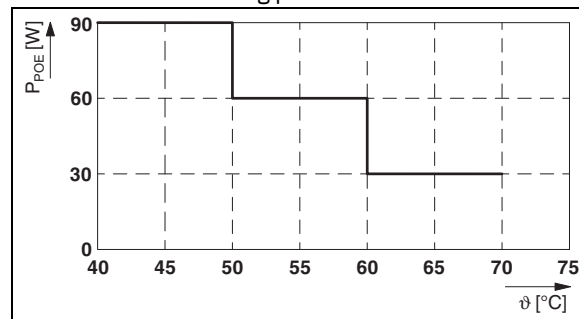


Bild 8-2 Derating pro Port



Konformität/Zulassungen

CE

CE-konform

UL, USA / Kanada

Listed

UL 61010-1, 3rd Edition

UL 61010-2-201, 2nd Edition

CAN/CSA C22.2 No. 61010-1-12

CSA C22.2 No. 61010-2-201:18

Schadgastest

ISA-S71.04-1985 G3 Harsh Group A

Konformität zur EMV-Richtlinie 2014/30/EU**Störfestigkeit nach EN 61000-6-2**

Entladung statischer Elektrizität	EN 61000-4-2	
	Kontakt-entladung	± 6 kV
	Luftentladung	± 8 kV
	Indirekte Entladung	± 6 kV
	Bemerkung	Kriterium B
Elektromagnetisches HF-Feld	EN 61000-4-3	
	Frequenzbereich	80 MHz ... 3 GHz (80 % Amplitudenmodulation mit 1 kHz)
	Feldstärke	10 V/m
	Bemerkung	Kriterium A
Schnelle Transienten (Burst)	EN 61000-4-4	
	Eingang	± 2,2 kV (1 Minute)
	Signal	± 2,2 kV (1 Minute)
	Bemerkung	Kriterium B
Stoßstrombelastungen (Surge)	EN 61000-4-5	
	Eingang	± 1 kV (AC-Versorgung, Leitung gegen Leitung) ± 2 kV (AC-Versorgung, Leitung gegen Erde)
Leitungsgeführte Beeinflussung	EN 61000-4-6	
	Frequenzbereich	0,15 MHz ... 80 MHz (80 % Amplitudenmodulation mit 1 kHz)
	Spannung	10 V
	Bemerkung	Kriterium A

Störaussendung

Störabstrahlung	EN 61000-6-4, Klasse B, Einsatzgebiet Wohn- und Kleingewerbebereich
Leitungsgeführte Störaussendung	EN 61000-6-3 Klasse B, Einsatzgebiet Wohn- und Kleingewerbebereich

Kriterium A Normales Betriebsverhalten innerhalb der festgelegten Grenzen

Kriterium B Vorübergehende Beeinträchtigung des Betriebsverhaltens, die das Gerät selbst wieder korrigiert

8.3 Abmessungen

Bild 8-3 Abmessungen

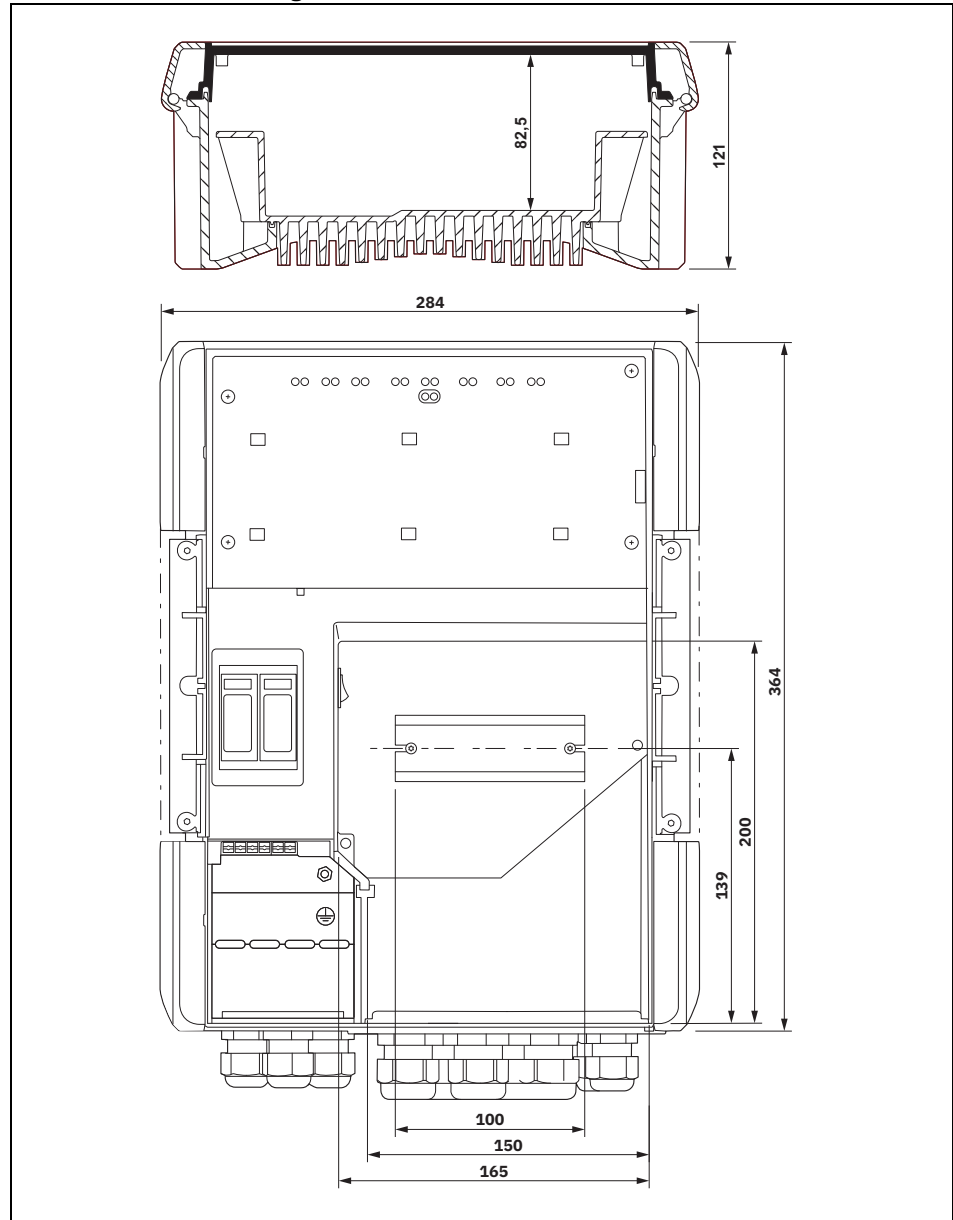
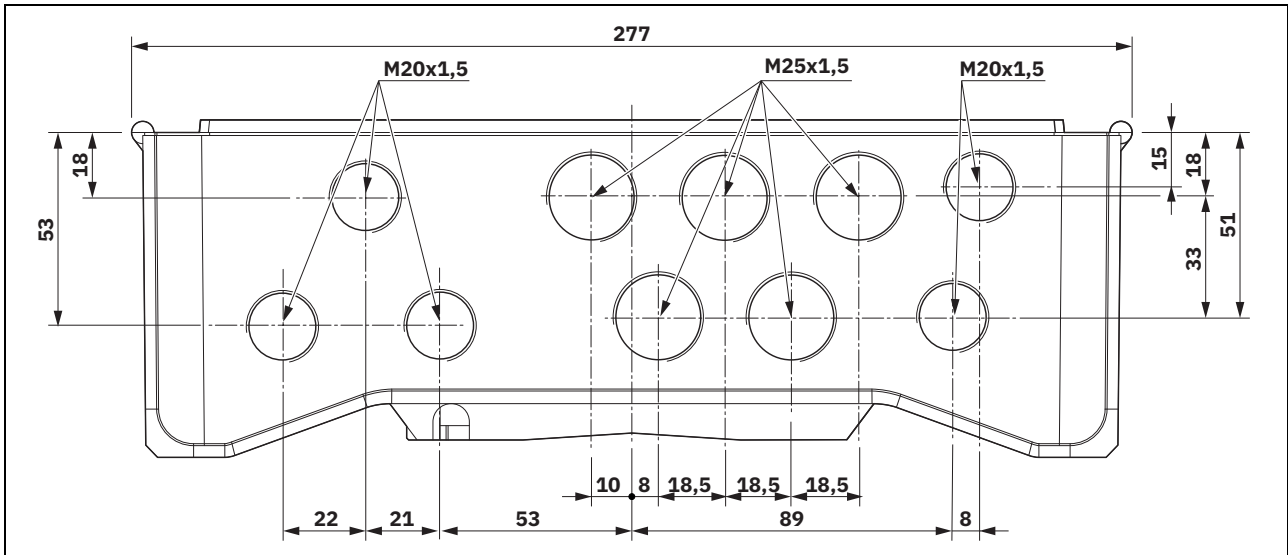
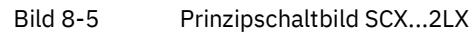


Bild 8-4 Abmessungen Unterseite



Phoenix Contact 91 / 118



A Technischer Anhang

A 1 Frame-Switching

Der Switch arbeitet im Store-and-Forward-Modus. Während er ein Datenpaket empfängt, analysiert der Switch die Quell- und Zieladressen. In seiner Adresstabelle speichert der Switch bis zu 8192 MAC-Adressen.

A 1.1 Store-and-Forward

Alle Datentelegramme, die der Switch empfängt, werden gespeichert und auf ihre Gültigkeit geprüft. Ungültige oder fehlerhafte Datenpakete (z. B. CRC-Fehler) sowie Fragmente (<64 Byte) werden verworfen. Gültige Datentelegramme leitet der Switch weiter.

A 1.2 Multiadressfähigkeit

Der Switch lernt alle Quelladressen je Port. Nur folgende Pakete werden über den betroffenen Port weitergeleitet:

- Unbekannte Quelladresse im Zieladressfeld
- Quelladresse dieses Ports im Zieladressfeld
- Multi- oder Broadcast-Adresse im Zieladressfeld

Der Switch kann bis zu 8192 Adressen lernen. Dies wird notwendig, wenn an einem oder an mehreren Ports mehr als ein Endgerät angeschlossen ist.

Sie können mehrere eigenständige Subnetze an einen Switch anschließen.

Adressen lernen

Der Switch erlernt selbstständig die Adressen der Endgeräte, die über diesen Port angeschlossen sind. Dazu wertet er die Quelladressen in den Datentelegrammen aus.

Wenn der Switch ein Datentelegramm empfängt, dann leitet er dieses nur an den Port weiter, über den der gewünschte Teilnehmer zu erreichen ist (falls die Adresse zuvor gelernt wurde).

Der Switch überwacht das Alter der gelernten Adressen. Adresseinträge, die ein bestimmtes Alter (Aging-Time) überschreiten, löscht der Switch selbstständig aus seiner Adresstabelle.



Bei Neustart werden alle gelernten Adresseinträge gelöscht. Bei Link-Down werden alle Einträge des betroffenen Ports gelöscht.



Eine Liste der erkannten MAC-Adressen finden Sie in der MAC-Adresstabelle.



Die Aging-Time stellen Sie über das MIB-Objekt „dot1dTpAgingTime“ (OID 1.3.6.1.2.1.17.4.2) ein.

A 1.3 Priorisierung

Um die interne Reihenfolge der Paketabarbeitung zu beeinflussen, unterstützt der Switch acht Priority Queues (Traffic Classes nach IEEE 802.1Q). Die Zuordnung von empfangenen Datentelegrammen zu diesen Klassen erfolgt durch die im VLAN-/Prioritätstag enthaltene Priorität des Datenpakets:

- 0 = niedrigste Priorität
- 7 = höchste Priorität

Bearbeitungsregeln

Der Switch-Controller leitet empfangene Pakete nach folgenden Entscheidungen in die zur Verfügung stehenden Empfangs-Queues:

- BPDU-Pakete werden immer in die hochpriori Queue eingeordnet.
- Pakete mit VLAN-/Prioritätstag werden entsprechend den oben genannten Queues weitergeleitet.
- Alle verbleibenden Daten werden in die niederpriori Queue eingeordnet.

Class-of-Service, CoS

Class-of-Service beschreibt einen Mechanismus, um den Wert des Prioritätsfelds (1 ... 7) in VLAN-Datenpaketen mit Tag zu berücksichtigen. Der Switch ordnet die Datenströme in verschiedene Abarbeitungs-Queues ein, abhängig davon, welche Prioritätsinformation im CoS-Tag enthalten ist. Der Switch unterstützt acht interne Abarbeitungs-Queues.

Quality-of-Service, QoS

Quality-of-Service beeinflusst Datenströme bei der Weiterleitung und behandelt dabei einzelne Datenströme anders, in der Regel bevorzugt. Mit QoS können Sie z. B. einzelnen Datenströmen eine Übertragungsbandbreite garantieren. Der Switch verwendet QoS in Verbindung mit der Priorisierung.

A 2 RSTP - Rapid Spanning Tree Protocol

Loops

Das RSTP-Protokoll ermöglicht Ethernet-Netzwerke mit redundanten Datenpfaden. Diese Netzwerke bilden eine vermaschte Topologie mit zunächst unzulässigen Schleifen (Loops). Die Loops führen dazu, dass Datenpakete endlos im Netzwerk kreisen oder auch dupliziert werden können. Die Folge ist eine Überlastung des Netzwerks durch kreisende Datenpakete. Die Kommunikation wird unterbrochen.

Deswegen wird die vermaschte Struktur mit Hilfe des Rapid-Spanning-Tree-Algorithmus durch einen logischen, deterministischen Pfad ersetzt. Der Pfad hat die Form einer Baumstruktur, die keine Loops mehr enthält. Wenn Datenpfade ausfallen, werden die vorher abgeschalteten Verbindungen teilweise wieder zugeschaltet. So wird das Netzwerk unterbrechungsfrei betrieben.

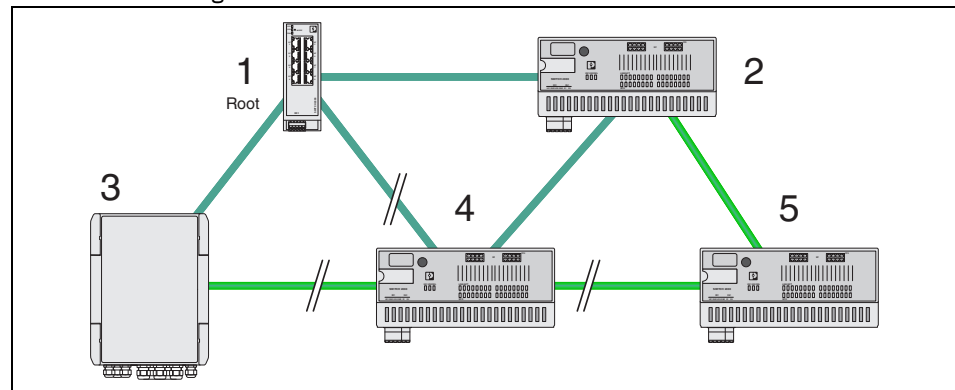
IEEE 802.1D-2004

Das RSTP-Protokoll ist in der IEEE 802.1D-2004 standardisiert. RSTP ist ereignisgesteuert. Dadurch sind die Umschaltzeiten deutlich kürzer als beim timerbasierten STP.

Beispiel

Um bei Ausfall eines Datenpfads weiterhin alle Teilnehmer im Netz erreichen zu können, gibt es in der folgenden Netzwerktopologie sechs redundante Pfade. Diese redundanten Pfade sind unzulässige Loops. Das RSTP-Protokoll überführt diese Topologie automatisch durch Abschalten ausgewählter Ports in einen Baum. Dabei ist ein Switch die Wurzel des Baums (Root-Bridge). Von der Root-Bridge aus ist jeder andere Switch über genau einen Datenpfad erreichbar.

Bild A-1 Mögliche Baumstruktur mit RSTP



Root-Bridge

Der Switch mit der niedrigsten Bridge Priority ist die Root-Bridge. Wenn die Root-Bridge ausfällt, wird anhand der Bridge Priority die nächste Root-Bridge gewählt. Wenn zwei Switches den gleichen Bridge-Priority-Wert aufweisen, wird die Root-Bridge anhand der niedrigeren MAC-Adresse gewählt.

BPDU

Die Root-Bridge sendet ständig BPDUs (Bridge Protocol Data Units) im Abstand der Hello-Time. Wenn eine Topologieänderung erkannt wird, werden Alternativpfade berechnet.

Hello-Time

Die Hello-Time ist der zeitliche Abstand, in dem die Root-Bridge BPDUs versendet.

- Standardeinstellung: 2 Sekunden

Pfadkosten

Anhand der Pfadkosten wird entschieden, welche Ports blockiert und welche bevorzugt werden. Die Pfadkosten werden nach der Bandbreite automatisch ermittelt. Sie können aber auch manuell einen Wert festlegen.

A 2.1 Port-Rollen

Root-Port

Der Root-Port verbindet einen Switch direkt oder über einen anderen Switch (Designated Switch) mit der Root-Bridge.

Designated Port

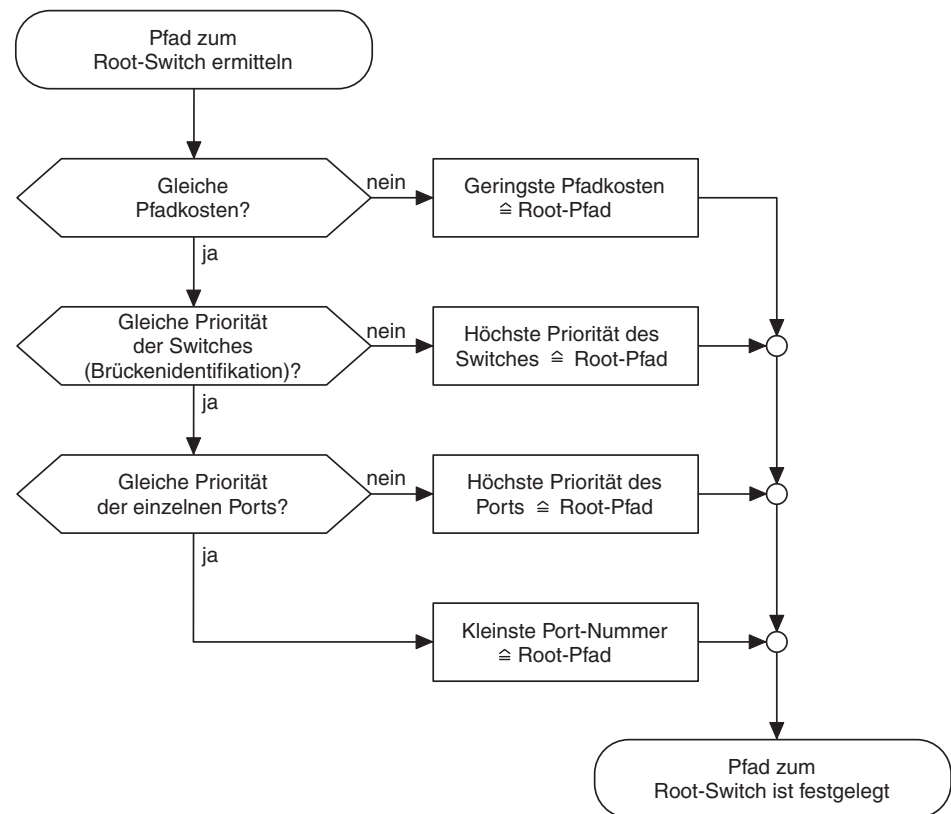
Der Designated Port ist ein Port an einem Designated Switch, der mit dem Root-Port des nächsten Switches verbunden ist.

Alternate-Port

Der Alternate-Port könnte ein Weg zur Root sein, er wurde aber nicht als Root-Port gewählt. Der Alternate-Port nimmt nicht an der aktiven Topologie teil.

A 2.2 Ablaufdiagramm zur Bestimmung des Root-Pfads

Bild A-2 Ablaufdiagramm zur Bestimmung des Root-Pfads



A 2.3 Port-Status

Discarding

Der Port ist geblockt, da er ansonsten ein Loop verursachen würde. Der Port empfängt und sendet keine Nutzerdaten, nur BPDU-Daten werden noch empfangen. Wenn ein Link ausfällt, wechselt der geblockte Port in den Status „Forwarding“.

Forwarding

Normaler Betrieb: Der Port empfängt Frames und leitet sie weiter. Die BPDUs werden überwacht.

A 2.4 Verbinden der Switches zu einer vermaschten Topologie

Nachdem Sie Rapid Spanning Tree bei allen Switches eingeschaltet haben, können Sie eine vermaschte Topologie mit redundanten Datenpfaden aufbauen. Sie können jetzt beliebige Datenverbindungen herstellen, ohne dabei auf die Entstehung von Loops zu achten. Sie können auch absichtlich Loops hinzufügen, um redundante Verbindungen herzustellen.

Ein Datenpfad zwischen Rapid-Spanning-Tree-Switches kann dabei sein:

- Eine direkte Verbindung.
- Eine Verbindung über einen oder mehrere weitere Switches, die kein Spanning Tree unterstützen.



Falls nicht alle eingesetzten Switches Spanning Tree unterstützen: Die Rekonfigurationszeit des Spanning Trees verlängert sich um die Aging-Time der Switches ohne Spanning-Tree-Unterstützung.

Darüber hinaus kann ein Datenpfad auch aus der Verbindung eines Spanning-Tree-Switches zu Folgendem bestehen:

- Einem Endgerät
- Einem aus mehreren Infrastrukturkomponenten ohne Spanning-Tree-Unterstützung bestehenden Netzwerksegment. In diesem Netzwerksegment dürfen **keine** Loops auftreten.

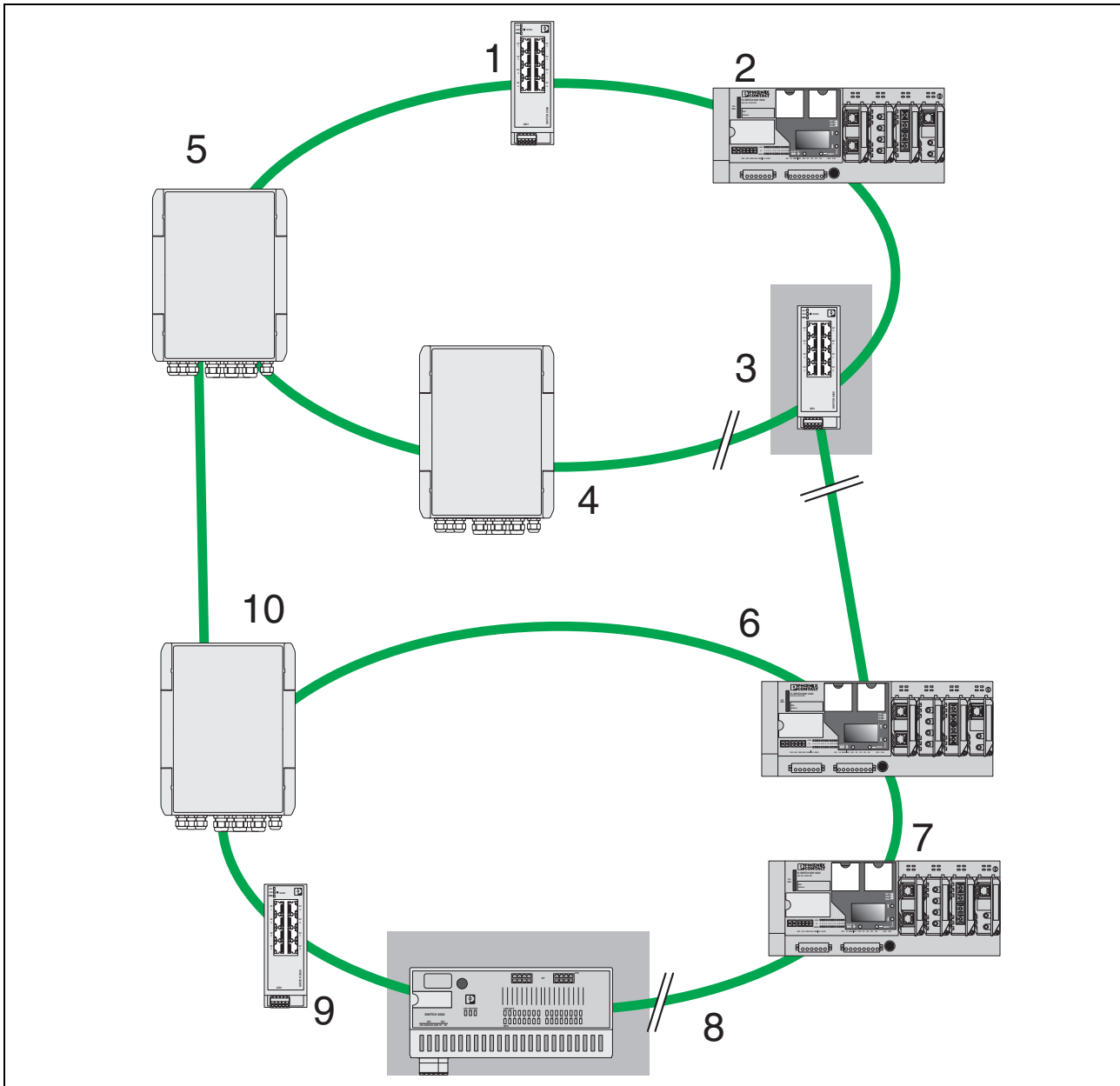
Wenn Sie Infrastrukturkomponenten ohne Rapid-Spanning-Tree-Unterstützung einsetzen möchten, z. B. Unmanaged Switches, beachten Sie folgende Regeln:

- **Regel 1: Rapid-Spanning-Tree-Transparenz aller Infrastrukturkomponenten**
Alle eingesetzten Infrastrukturkomponenten in Ihrem Netzwerk, die Rapid Spanning Tree nicht aktiv unterstützen, müssen transparent für Rapid-Spanning-Tree-Nachrichten (BPDUs) sein. Diese müssen BPDUs unverändert an alle Ports weiterleiten. Der Switch ist bei abgeschaltetem Spanning Tree transparent für BPDUs.
- **Regel 2: Mindestens eine aktive Rapid-Spanning-Tree-Komponente pro Loop**
Eine aktive Rapid-Spanning-Tree-Komponente unterstützt das Rapid-Spanning-Tree-Protokoll, sendet und empfängt BPDUs, wertet sie aus und setzt seine Ports in die entsprechenden RSTP-Zustände.
Um den Loop aufzulösen, muss in jedem Loop eines Netzwerks mindestens eine aktive Rapid-Spanning-Tree-Komponente vorhanden sein.

A 2.5 Beispieltopologie

In diesem Beispiel sind zwei Netzwerksegmente über redundante Datenpfade miteinander verbunden. Zwei RSTP-Komponenten haben Ports im Zustand „Blocking“ (grau hinterlegt). Das ist ausreichend, um das Netzwerk zu betreiben.

Bild A-3 Redundante Kopplung von Netzsegmenten



A 2.6 Erweiterte Konfiguration

Es kann sinnvoll sein, die Topologie, die sich durch RSTP ausbildet, nicht den zufälligen MAC-Adressen der beteiligten Switches zu überlassen, sondern diese aktiv vorzugeben. So können Sie z. B. Einfluss auf die nichtblockierenden und blockierenden Datenpfade nehmen und somit eine Lastverteilung vorgeben.

Festlegen des Root-Switches

- Stellen Sie auf der Seite „Network Redundancy“ unter „Bridge Priority“ den kleinsten Wert ein (höchste Priorität).
- Stellen Sie sicher, dass für alle anderen Switches im Netzwerk ein höherer Wert eingestellt ist (geringere Priorität). Die eingestellten Pfadkosten werden hierbei nicht bewertet.

Festlegen des Root-Ports bzw. Designated Ports

Der Root-Port und der Designated Port sind immer die Ports, die die geringsten Pfadkosten ausweisen. Bei Kostengleichheit entscheidet die Priorität. Wenn diese auch identisch ist, entscheidet die Port-Nummer.

- Stellen Sie auf der Seite „Network Redundancy“ für den Port eine geeignete Kombination aus Kosten und Priorität ein.
- Stellen Sie sicher, dass alle anderen Switches des Netzwerks höhere Kosten oder eine kleinere Priorität (größerer Zahlenwert) haben.

Abschalten von RSTP

Wenn RSTP abgeschaltet ist, wird an diesem Port die Fast-Forwarding-Funktion genutzt.

Um RSTP abzuschalten, muss eine der folgenden Bedingungen erfüllt sein:

- An dem Port ist ein Endgerät angeschlossen.
- An dem Port sind weitere Infrastrukturkomponenten angeschlossen. In dem entsprechenden Netzsegment sind keine Loops.
- An dem Port sind weitere Infrastrukturkomponenten angeschlossen, die einen eigenen Rapid Spanning Tree bilden. Zu diesem Netzsegment darf keine weitere redundante Verbindung bestehen.

Änderung der Protokoll-Timer



ACHTUNG: Fehlfunktion

Wenn Sie die Protokoll-Timer ändern, kann das zu instabilen Netzwerken führen.

Wenn Sie z. B. mehr als 20 aktive Rapid-Spanning-Tree-Komponenten in einer Ringtopologie einsetzen, kann es erforderlich sein, die Protokoll-Timer zu verändern. Ebenso können Sie versuchen, durch eine Änderung der Timer die Rekonfigurationszeiten zu verkürzen. Gehen Sie dabei jedoch vorsichtig vor, um instabile Netze zu vermeiden.

Die Protokollzeiten werden vom Root-Switch vorgegeben und über BPDU an alle Teilnehmer verteilt. Es reicht also zunächst aus, die Werte nur im Root-Switch zu ändern. Wenn der Root-Switch ausfällt, werden die Timer-Werte eines anderen aktiven RSTP-Switches (des neuen Root-Switches) für das gesamte Netzsegment gültig. Beachten Sie dieses Verhalten beim Konfigurieren Ihrer Komponenten.

Einstellen der Timer-Werte

- Maximale Anzahl der aktiven Rapid-Spanning-Tree-Komponenten entlang eines Pfads vom Root-Switch aus:
 $(\text{MaxAge} / 2) - \text{Hello-Time} + 1$
- Wenn Sie z. B. die MaxAge auf 40 Sekunden setzen, erhöhen Sie die maximale Distanz einer Infrastrukturkomponente von der Root-Bridge auf 19 Hops. Damit erhöht sich die maximal mögliche Anzahl Geräte in einer Ringtopologie.
 $\text{MaxAge} \geq 2 \times \text{Hello-Time} + 1 \text{ s}$

A 2.7 Fast Ring Detection

Sie aktivieren die Funktion „Fast Ring Detection“ im Web-based Management unter „[Network Redundancy](#)“.

Diese Funktion beschleunigt das Umschalten auf einen redundanten Pfad im Fehlerfall und ermöglicht eine einfache Diagnose. Durch die Fast Ring Detection wird jedem Ring eine ID zugewiesen. Diese ID wird jedem Switch in dem jeweiligen Ring bekannt gemacht. Ein Switch kann gleichzeitig mehreren unterschiedlichen Ringen angehören.

i Die Funktion „Fast Ring Detection“ ist proprietär. Sie ist nur möglich, wenn alle Geräte in der Struktur die Funktion unterstützen.

Aufbau der Ring-ID

Die Ring-ID bildet sich aus der Port-Nummer des blockierenden Ports und der MAC-Adresse des zugehörigen Switches.

Vorteile der Ring-ID:

- Redundante Wege werden leichter identifiziert
- Blockierende Ports werden leichter gefunden
- Kontrolle, ob die Wunschtologie der tatsächlichen Topologie entspricht

Beachten Sie bei Fast Ring Detection Folgendes:

- Verwenden Sie bei RSTP Fast Ring Detection nur Geräte, die diese Funktion unterstützen.
- Schalten Sie die RSTP Fast Ring Detection auf **allen** Geräten ein.
- Alle Datenpfade müssen im Vollduplexbetrieb sein.

Umschaltzeiten von Fast Ring Detection

Bei der maximal zulässigen Anzahl von Switches in einem Ring ergeben sich mit Fast Ring Detection typische Umschaltzeiten von 100 bis 300 ms.

i Die maximale Anzahl von Switches erreichen Sie nur, wenn Sie gleichzeitig „Large Tree Support“ aktivieren.

A 2.8 Large Tree Support

Durch die Funktion „Large Tree Support“ wird die maximal mögliche Anzahl Switches in einer RSTP-Topologie vergrößert.

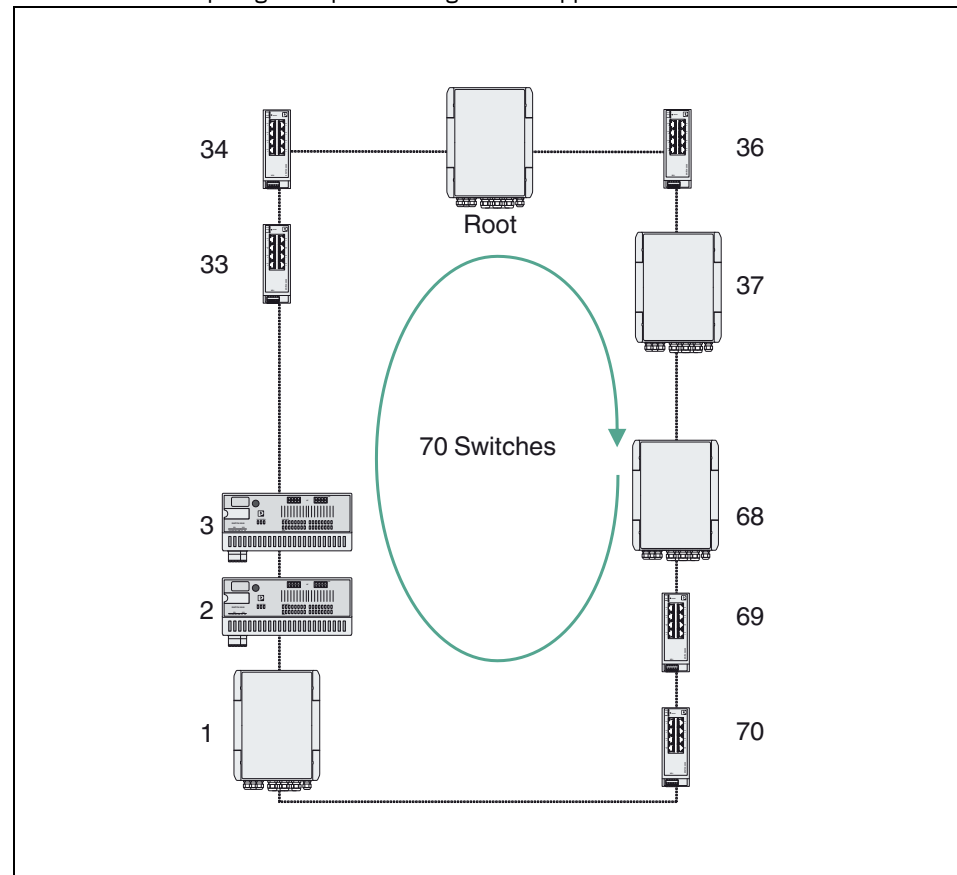
Eigenschaften Large Tree Support

Die Funktion „Large Tree Support“ ist proprietär. Sie ist nur möglich, wenn alle Geräte in der Struktur die Funktion unterstützen.

Beachten Sie bei Large Tree Support:

- Verwenden Sie in der Topologie nur Geräte, die den Large Tree Support unterstützen.
- Schalten Sie Large Tree Support an **allen** Geräten ein.
- Wir empfehlen, Large Tree Support nur zu aktivieren, wenn Ihr Netzwerk mehr Switches umfasst, als das Standard-RSTP ermöglicht.

Bild A-4 Topologiebeispiel für Large Tree Support



A 2.9 Topologiegrößen

Das RSTP-Protokoll erlaubt den Aufbau redundanter Netzwerke in Ringtopologien oder vermaschten Strukturen.

Mit der Smart Ethernet Box können Sie RSTP nach IEEE 802.1D-2004 in diesen Netzwerken einsetzen. Um Ausfälle zu vermeiden, müssen Sie bei der Planung und dem Aufbau die folgenden Maximalwerte einhalten.

Tabelle A-1 Maximalwerte bei RSTP

	Large Tree Support deaktiviert		Large Tree Support aktiviert	
	Standard-einstellung, MaxAge = 20	MaxAge = 40	Standard-einstellung, MaxAge = 20	MaxAge = 40
Ring	20 Geräte im Ring	40 Geräte im Ring	70 Geräte im Ring	❗ Nicht empfohlen. Wenn Large Tree Support aktiviert ist, verwenden Sie die Standardeinstellungen
Vermascht	Distanz zur Root-Bridge 9 Hops	Distanz zur Root-Bridge 19 Hops	Distanz zur Root-Bridge 34 Hops	

A 3 SNMP - Simple Network Management Protocol

SNMP ist ein herstellerneutraler Standard für das Netzwerkmanagement. Er definiert Kommandos zum Lesen und Schreiben von Informationen und Formate von Fehler- und Statusmeldungen. Außerdem bietet SNMP ein strukturiertes Modell. Es besteht aus Agenten mit ihrer jeweiligen MIB (Management Information Base) und einem Manager. Der Manager ist eine Software, die auf einer Netzwerk-Managementstation ausgeführt wird.

Management Information Base (MIB)

Beschreibung, in die alle Daten (Objekte und Variablen) eingetragen werden, die zum Netzwerkmanagement benötigt werden.

Agent

Die Agenten befinden sich innerhalb von Switches, Busklemmen, Routern und anderen Geräten, die SNMP unterstützen. Die Aufgabe der Agenten ist das Sammeln und Bereitstellen von Daten in der MIB.

Manager

Der Manager fordert diese Informationen regelmäßig an und stellt sie dar. Mit Daten, die vom Manager in die MIB geschrieben werden, ist eine Konfiguration der Geräte möglich. In dringenden Fällen können die Agenten auch Meldungen (Traps) direkt an den Manager schicken.

Traps

Traps sind spontane SNMP-Alarm- oder Informationsmeldungen, die ein SNMP-fähiges Gerät aufgrund von besonderen Ereignissen versendet. Die Traps werden mit höchster Priorität ggf. an unterschiedliche Adressen übertragen. Die Traps können anschließend im Klartext von der Managementstation dargestellt werden. Die Empfänger-IP-Adressen (Trap-Targets/Receiver) dieser Traps müssen Sie auf dem jeweiligen Gerät einstellen.



Bei allen Bedienoberflächen (außer bei SNMPv3) ist das voreingestellte Passwort private.



Bei SNMPv3 muss das Passwort mindestens acht Zeichen lang sein. Wenn das Default-Passwort „private“ eingestellt ist, müssen Sie für den Zugriff „private_“ verwenden. Bei SNMP V1/2 sind Passwörter nicht erforderlich.



Alle Konfigurationsänderungen, die nach einem Neustart des Geräts wirksam sein sollen, müssen Sie mit Hilfe des Objekts „flWorkFWCtrlConfSave“ dauerhaft speichern.

Nicht alle Geräte unterstützen alle Objektklassen. Die Abfrage einer nicht unterstützten Objektklasse liefert eine Fehlermeldung. Der Versuch, eine nicht unterstützte Objektklasse zu ändern, hat ebenfalls eine Fehlermeldung zur Folge.

Die Beschreibungen der einzelnen SNMP-Objekte sind in den jeweiligen MIBs. Sie können diese unter phoenixcontact.com/products herunterladen. Sie finden die MIB im jeweiligen Software-Paket (zip-File) einer Firmware.

SNMP-Schnittstelle

Der SNMP-Agent verwaltet die folgenden MIBs (Management Information Base):

- FL Managed Infrastructure MIB
- lldpMIB
- RFC1213 MIB
- rmon
- snmpMIB
- ifMIB
- snmpFrameworkMIB
- etherMIB
- pBridgeMIB
- qBridgeMIB
- dot1dBridge
- rstpMIB
- IP MIB

Für die Smart Ethernet Box benötigen Sie folgende MIB:

- FL-MGD-SURVEILLANCE-MIB (Dateiname: FL-MGD-SURVEILLANCE-MIB_Rel101)

Über SNMP können Netzwerkmanagement-Stationen, wie z. B. ein PC mit einem MIB-Browser, Konfigurations- und Diagnosedaten der Netzwerk-Teilnehmer auslesen und verändern.

Sie können auch beliebige SNMP-Tools oder Netzwerkmanagement-Tools für den Zugriff auf Factoryline-Produkte nutzen. Dazu sind die von dem jeweiligen Gerät unterstützten MIBs den SNMP-Management-Tools zur Verfügung zu stellen.

Zum einen sind dies weltweit gültige MIBs, die in RFCs (Request for comments) festgelegt und beschrieben sind. Dazu zählt z. B. die MIB2 nach RFC1213. Sie wird von jedem SNMP-fähigen Netzwerk-Teilnehmer unterstützt. Zum anderen kann jeder Hersteller eigene private SNMP-Objekte festlegen, die dann in dem großen SNMP-Objekt-Baum in einem privaten Herstellerbereich eingeordnet werden. Für diesen privaten (enterprise) Bereich ist dann jeder Hersteller selbst verantwortlich. Einer Objekt-ID darf z. B. nur einmalig ein Objekt (Objektname und Parameter) zugewiesen und veröffentlicht werden. Wenn dieses Objekt danach nicht mehr benötigt wird, so wird es als auslaufend gekennzeichnet. Es wird unter keinen Umständen z. B. mit anderen Parametern erneut verwendet.

Die ASN1-SNMP-Objekte werden von Phoenix Contact durch die Veröffentlichung der Beschreibung auf den Internetseiten bekannt gegeben.

Das Lesen der SNMP-Objekte ist nicht durch ein Passwort geschützt. Sie müssen im SNMP beim lesenden Zugriff ein Passwort eingeben, dieses ist aber auf „public“ eingestellt. Sie können es nicht verändern. Im Auslieferungszustand ist das Passwort für den Schreibzugriff „private“. Der Anwender kann das Passwort verändern.



SNMP und Webinterface verwenden dasselbe Passwort. Der Anwender kann das Passwort verändern.

SNMPv3

Wenn Sie SNMPv3 nutzen, müssen Sie beim Zugriff auf die SNMP-Objekte einige Punkte beachten. SNMPv3 ist im Gegensatz zu SNMPv2 ein gesichertes Protokoll, bei dem die Inhalte der Nachrichten sowie Passwörter verschlüsselt übertragen werden.

Um SNMPv3 zu nutzen, müssen Sie zunächst das Gerät entsprechend konfigurieren (siehe „[SNMP](#)“ auf Seite 63). Zusätzlich müssen Sie Ihren MIB-Browser auf SNMPv3 umstellen und einen SNMPv3 User mit folgenden Parametern anlegen:

- MD5 als Algorithmus für Authentication
- DES als Algorithmus für Privacy
- Username: admin
- Passwort: aktuelles Gerätepasswort

Das Passwort muss mindestens acht Zeichen lang sein. Wenn das Default-Passwort „private“ eingestellt ist, müssen Sie für den Zugriff „private_“ verwenden.

A 4 LLDP - Link Layer Discovery Protocol

Das Link Layer Discovery Protocol dient Netzwerk-Teilnehmern dazu, die eigenen Nachbarschaftsbeziehungen zu erlernen und zu pflegen. Der Switch unterstützt LLDP nach IEEE 802.1ab und ermöglicht so eine Topologieerkennung von Geräten, bei denen ebenfalls LLDP aktiviert ist.

Vorteile von LLDP:

- Verbesserte Fehlerorterkennung
- Verbesserter Gerätetausch
- Effiziente Netzwerkprojektierung

Wenn LLDP aktiviert ist, werden folgende Informationen empfangen oder versendet:

- Das Gerät versendet die eigenen Management- und Verbindungsinformationen an benachbarte Geräte.
- Das Gerät empfängt Management- und Verbindungsinformationen von benachbarten Geräten.



Ein Port, der durch RSTP blockiert ist, empfängt keine LLDP-BPDUs. Er versendet sie aber.

Funktion

Eine Netzwerk-Infrastrukturkomponente sendet zur Verbreitung von Topologieinformationen im zeitlichen Abstand vom „Message Transmit Interval“ an jedem Port eine Port-bezogene BPDU (Bridge Protocol Data Unit). Sie enthält die eigenen Geräteinformationen.

Durch diese BPDUs erlernt die angeschlossene Gegenstelle Port-bezogen die jeweiligen Nachbarschaftsinformationen. Die erlernten Informationen werden für eine definierte Zeitspanne gespeichert (TTL, Time To Live). Wenn die gleichen BPDUs erneut empfangen werden, wird der TTL-Wert wieder erhöht. Die Information bleibt dadurch gespeichert. Wenn die TTL abläuft, wird die Nachbarschaftsinformation gelöscht.



Der Switch verwaltet maximal 50 Nachbarschaftsinformationen. Darüber hinausgehende Informationen werden ignoriert.



Falls an einem Switch-Port mehrere Nachbarn angezeigt werden: Zwischen diesem Switch und den angezeigten Nachbarn ist mindestens ein weiterer Switch installiert, der LLDP nicht unterstützt oder nicht aktiviert hat.

Tabelle A-2 Ereignistabelle bei LLDP

Ereignis	Aktion des eigenen LLDP-Agenten	Reaktion des LLDP-Agenten des Nachbarn
LLDP-Agent aktivieren oder Gerätestart	LLDP-BPDUs an allen Ports versenden	Absender in die Liste der Nachbarn aufnehmen
LLDP-Agent deaktivieren oder Software-Reset	LLDP-BPDUs mit einem TTL-Wert von 0 Sekunden an allen Ports versenden	Absender aus der Liste der Nachbarn löschen
Link-Up	Port-bezogene LLDP-BPDUs senden	Absender in die Liste der Nachbarn aufnehmen
Link-Down	Alle Nachbarn dieses Ports löschen	-
Timer (Message Transmit Interval)	Zyklisches Senden der BPDUs an allen Ports	Informationen aktualisieren
Aging (Time To Live)	Nachbarschaftsinformation löschen	-
Empfang einer BPDU von einem neuen Nachbarn	Nachbarschaftsliste erweitern, mit Port-bezogener BPDU antworten	Absender in die Liste der Nachbarn aufnehmen

B Verzeichnisanhang

B 1 Abbildungsverzeichnis

Bild 1-1:	QR-Code scannen	11
Bild 3-1:	Smart Ethernet Box mit LWL-Anschlüssen	16
Bild 3-2:	Smart Ethernet Box mit RJ45-Anschlüssen	18
Bild 3-3:	Rückseite	20
Bild 3-4:	Zonen in der Smart Ethernet Box	20
Bild 3-5:	Gehäuse öffnen	21
Bild 4-1:	Montageadapter, Mastmontage	23
Bild 4-2:	Beispiel Mastmontage, Ø 50 ... 90 mm	23
Bild 4-3:	Montageadapter, Wandmontage	24
Bild 4-4:	Befestigungslöcher zur Wandmontage	25
Bild 4-5:	Spleißkassette entnehmen	26
Bild 4-6:	Schraube der Flanschplatte lösen	27
Bild 4-7:	Flanschplatte herausziehen	27
Bild 4-8:	Schirmblech herausbrechen	28
Bild 4-9:	Demontieren	29
Bild 4-10:	Kabelverschraubungen	31
Bild 4-11:	Kabelverschraubung M20 montieren	33
Bild 4-12:	Kabelverschraubung M25 montieren	33
Bild 4-13:	Versorgungsspannung anschließen	34
Bild 4-14:	1 = Netzspannungszone / 2 = Kleinspannungszone	34
Bild 4-15:	SFP-Modul	35
Bild 4-16:	LWL-Kabel abmanteln, Kabelverschraubung M20	36
Bild 4-17:	LWL-Kabel einführen	36
Bild 4-18:	3,5-mal durch die Spleißkassette führen	37
Bild 4-19:	Pigtail anschließen (3-mal durch die Spleißkassette führen)	38
Bild 4-20:	SCX-DOOR-LOCK: Verriegelungslasche einhängen	40
Bild 4-21:	SCX-DOOR-LOCK: Türriegel montieren	40
Bild 5-1:	Basic Setup	43
Bild 5-2:	User Accounts, Add User	44
Bild 5-3:	User Roles, Add Role	45
Bild 5-4:	Time Settings	46
Bild 5-5:	Device Access	47
Bild 5-6:	Reboot Device & Factory Defaults	48

Bild 5-7:	Device Identification	49
Bild 5-8:	RADIUS Authentication	50
Bild 5-9:	Syslog	51
Bild 5-10:	Config Up/Download	52
Bild 5-11:	Firmware Update	53
Bild 5-12:	Network	54
Bild 5-13:	Ports	55
Bild 5-14:	Port Mirroring	56
Bild 5-15:	MAC Filter	57
Bild 5-16:	PoE	58
Bild 5-17:	PoE Watchdog	60
Bild 5-18:	Network Redundancy	61
Bild 5-19:	SNMP	63
Bild 5-20:	VLAN	64
Bild 5-21:	LLDP	65
Bild 5-22:	AUX Power	66
Bild 5-23:	Time Profile Scheduling	67
Bild 5-24:	Time Profile Scheduling, Time Profile Configuration Weekly	68
Bild 5-25:	Time Profile Assignment	69
Bild 6-1:	Module für Überspannungsschutz	77
Bild 6-2:	Überspannungsschutzmodule	77
Bild 8-1:	Derating (PoE-Leistung gesamt)	87
Bild 8-2:	Derating pro Port	87
Bild 8-3:	Abmessungen	89
Bild 8-4:	Abmessungen Unterseite	90
Bild 8-5:	Prinzipschaltbild SCX...2LX	91
Bild 8-6:	Prinzipschaltbild SCX...2T	91
Bild A-1:	Mögliche Baumstruktur mit RSTP	94
Bild A-2:	Ablaufdiagramm zur Bestimmung des Root-Pfads	95
Bild A-3:	Redundante Kopplung von Netzsegmenten	97
Bild A-4:	Topologiebeispiel für Large Tree Support	100

B 2 Tabellenverzeichnis

Tabelle 3-1:	Übersicht Produktvarianten.....	14
Tabelle 3-2:	LEDs SCX xPOE 2LX	17
Tabelle 3-3:	LEDs SCX xPOE 2T	19
Tabelle 5-1:	Revert, Apply, Save	42
Tabelle 5-2:	LEDs im Smart Mode	73
Tabelle 6-1:	Module für Überspannungsschutz.....	77
Tabelle A-1:	Maximalwerte bei RSTP	101
Tabelle A-2:	Ereignistabelle bei LLDP	105
Tabelle C-1:	Änderungsnachweis.....	114

B 3 Stichwortverzeichnis

A

Abmessungen	89
ACD Mode	54
Administration	44
Alarm	70
Allowed MAC Address	57
Anbauten	6
Anschließen	
Ethernet-Netzwerk	34
LWL-Kabel	35
Versorgungsspannung	34
Apply	42
Artikelnummer	81
Aufbau	
SCX xPOE 2LX	16
SCX xPOE 2T	18
Ausgang, 24 V	66
Auspacken	13
Authentifizierung	49

B

Backup-Root	61
Bandbreiten-Watchdog	60
Basic Setup	43
Benutzername	41
Benutzerverwaltung	44
Beschreibung	14
Bestelldaten	81
Bestimmungsgemäße Verwendung	6
Blockschaltbild	91
Bridge	61
Browser	41

C

CLI-Kommando	48
CLI-Service	48
Config Up/Download	54
Configuration	54

D

Datensicherheit	10
Demontageöffnung	20

Demontieren	22
SFP-Modul	29
Derating	87
Device Access	49
Device Management	49
Diagnose	70
Dichteinsatz	33
Dot1x Authenticator	50

E

Elektrischer Anschluss	30
Entsorgung	80
Erdung	32
Ereignis	70
Erlaubte MAC-Adresse	57
Event	70

F

Fast Ring Detection	61
Firmware-Update	53

G

Gehäuse schließen	40
Gerätedefekt	78
Gerätetausch	76
Überspannungsschutz	77
Geräteverwaltung	49
Gerätezugriff	49

H

HTTPS-Zertifikat	48
------------------------	----

I

Inbetriebnahme	39
Installieren	22
Instandhaltung	78
IP Address Assignment	43
IP-Adresse	43
IP-Adressvergabe	43
Isolationsmessung	80

K

Kabel vorbereiten	31
Kabelverschraubung	33
Klimamembran	20
Konfiguration laden	54
Konfigurieren	41
Kontrolle	39

L

Lagern	12
Large Tree Support.....	61
LEDs	
SCX xPOE 2LX	17
SCX xPOE 2T	19
Lichtwellenleiter-Kabel	35
Lieferung kontrollieren	13
Link Layer Discovery Protocol.....	65
Lizenzhinweise	15
LLDP	65
Local Diagnostics.....	72
Lokale Diagnose	72
LWL-Kabel	35

M

MAC-Adresse.....	57
MAC-Filter.....	57
Mastmontage.....	23
Mastschelle.....	23
Maßzeichnung.....	89
Meldeausgang	66
Montageadapter	
Mastmontage	23
Wandmontage	24
Montageort	22
Montieren	22

N

Network	54
Network Redundancy.....	61
Netzwerkkonfiguration.....	54
Netzwerksicherheit	10
Neustart	54

O

Open Source Software	15
----------------------------	----

Output	66
--------------	----

P

Passwort.....	41
Passwort (Voreinstellung)	41
Ping.....	60
PoE-Watchdog	60
Port Configuration	55
Port Mirroring	56
Portkonfiguration	55
Port-Tabelle	72
Power-over-Ethernet	58
Power-over-Ethernet-Watchdog.....	60
Power-Watchdog	60
Prinzipschaltbild	91
Produktbeschreibung	14
Produktvarianten	14

R

RADIUS Authentication	49
Rapid Spanning Tree.....	61
Reboot Device	54
Redundanz	61
Reparatur	78
Revert	42
Root-Bridge.....	61
RSTP	61
Rückseite.....	20
Rücksendung.....	13
Rücksetzen auf Werkseinstellungen	54

S

Save	42
Schaltausgang.....	66
Schaltbild	91
Schaltplan	91
SCX-DOOR-LOCK	40
Security Context.....	48
SFP-Modul.....	35
SFP-Slot.....	35
Sicherheit im Netzwerk.....	10
Sicherheitshinweise	5, 30
Sicherheitskontext	48
Simple Network Management Protocol	63
SNMP	63

SNTP-Server	46
Spannungsversorgung	
Siehe Versorgungsspannung	
Speichern	42
Spleißkassette	35
SSH	48
SSH-Zertifikat	48
Standort	22
Statische IP-Adresse	43
Synchronisierung	46

T

Technische Daten	83
Telnet	48
Temperaturbereich	87
Tragschiene	38
Transportieren	12
Transportschaden	13
Trap	63
Tür	40
Türriegel	40

U

Übersicht Produktvarianten	14
Überspannungsschutz	77
Umbauten	6
Umgebungsbedingungen	87
Update	53
User Management	44

V

VAL-MS	77
Veränderungen des Produkts	6
Verriegeln	40
Verriegelungslasche	40
Verschließen	40
Versorgungsspannung	34
Verwaltung	44
VLAN	64

W

Wandmontage	24
Wartung	79
Watchdog	60

Web-based Management	41
Starten	41
Webbrowser	41

Z

Zeit-Server	46
Zertifikate	48
Zu Ihrer Sicherheit	5
Zubehör	81
Zusätzliche Geräte installieren	38

C Änderungsnachweis

Tabelle C-1 Änderungsnachweis

Dokumentenrevision	Hardware-Revision	Firmware-Revision	Datum	Beschreibung
00	-	-	2020-04-08	Erstveröffentlichung
01	11	101	2020-11-03	Kapitel 1.6 "UL-Hinweise" eingefügt In Kapitel 4.3.1 Informationen zum Vorhängeschloss eingefügt Tabelle 6-1 "Module für Überspannungsschutz" eingefügt, Informationen zum Heavy-Duty-Überspannungsschutz In Kapitel 8.1.1 Zubehör ergänzt In Kapitel 8.2 Informationen zur UL-Zulassung eingefügt Kapitel 8.3 "Abmessungen" und Kapitel 8.4 "Prinzipschaltbild" eingefügt In Kapitel A3 Hinweis zu SNMPv3-Passwörtern korrigiert

Tabelle C-1 Änderungsnachweis

Dokumentenrevision	Hardware-Revision	Firmware-Revision	Datum	Beschreibung
02	-	111	2022-09-27	Kapitel 3.1 "Lizenzhinweise zu Open Source Software" erweitert Kapitel 4.1.3 "Wandmontage" erweitert Kapitel 5.1.2 "Basic Setup" aktualisiert (Änderungen im Web-based Management des Produkts) Kapitel 5.1.3 "Administration" aktualisiert, "User Accounts", "User Roles" und "Time Settings" hinzugefügt Kapitel 5.15 "Diagnostics" überarbeitet Kapitel 5.2.3 "Rücksetzen auf eine vorherige Firmware-Version" eingefügt Kapitel 7.2 "Entsorgung" erweitert In Kapitel 8.2 Daten zu Brennbarkeitsklasse, Brandschutz, Halogenfreiheit und Sonstige Beständigkeit eingefügt Kapitel A2 "RSTP - Rapid Spanning Tree Protocol" überarbeitet
03	-	-	2023-09-13	Umbenennung des Produkts von "Smart Camera Box" zu "Smart Ethernet Box" In Kapitel 1.1 Security-Piktogramm ergänzt Kapitel 1.7 "Sicherheit im Netzwerk" überarbeitet
04	21	111	2025-05-25	Neues Layout Im Kapitel 1.3.2 "Veränderungen des Produkts" den Absatz "Erweiterbare Kabelverschraubungen" eingefügt Kapitel 1.8 "Anwenderdokumentation" eingefügt Bild 3-1, 3-2, 8-3, 8-4 an die Hardware-Version 21 angepasst Kapitel 4.1.4 "Gehäuse ab Hardware-Version 21" eingefügt

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.

Dieses Handbuch ist einschließlich aller darin enthaltenen Abbildungen urheberrechtlich geschützt. Jegliche Veränderung des Inhaltes oder eine auszugsweise Veröffentlichung sind nicht erlaubt.

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.com/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