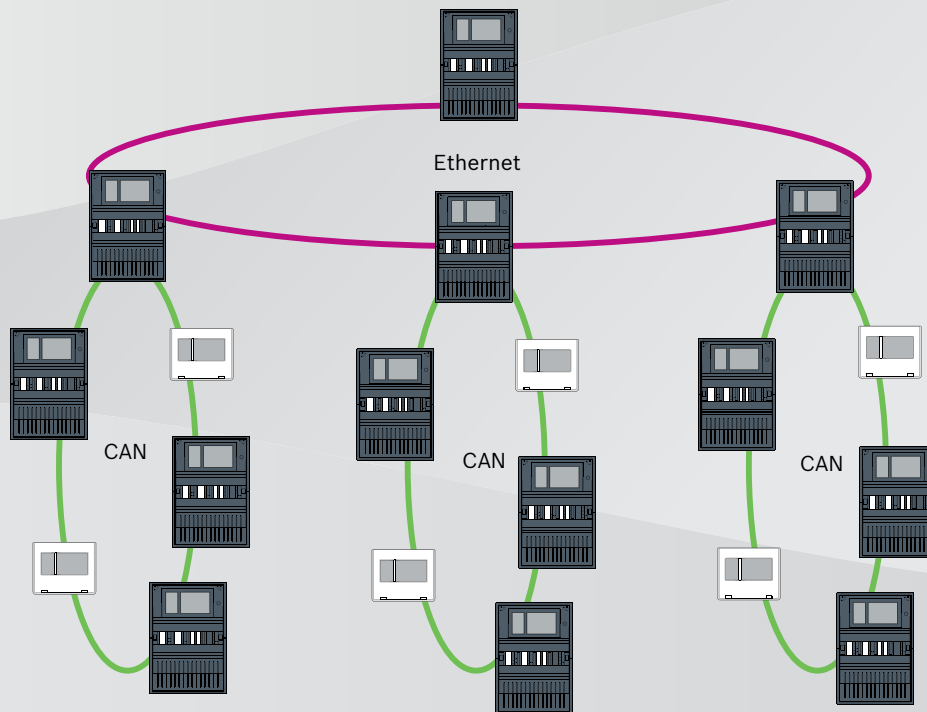


# AVENAR panel Serie | FPA-5000 | FPA-1200





# Inhaltsverzeichnis

<b>1</b>	<b>Sicherheit</b>	<b>5</b>
1.1	Organisatorische Maßnahmen für Rechner mit Service-Clients	5
1.2	Erläuterung der Sicherheitssymbole	6
1.3	Sicherheitshinweise	6
<b>2</b>	<b>Einführung</b>	<b>8</b>
<b>3</b>	<b>Systemübersicht</b>	<b>8</b>
<b>4</b>	<b>Topologien</b>	<b>10</b>
4.1	CAN-Ring	16
4.2	Ethernet-Ring	16
4.3	Ethernet-Ring mit OPC-Server	16
4.4	Ethernet-Ring mit OPC-Server an redundanter Zentrale	17
4.5	Ethernet/CAN Doppelring	17
4.6	CAN-Ring mit Ethernet-Segmenten	17
4.7	Ethernet-Backbone mit Sub-Ringen (Ethernet/CAN)	18
4.8	Anschalten von Ethernet-Ringen	20
<b>5</b>	<b>Ethernet-Netzwerk</b>	<b>21</b>
5.1	Protokolle	22
5.2	Netzwerkdurchmesser	22
5.3	Verwendete Kabel	24
5.4	Erstellen oder Ändern eines Ethernet-Netzwerks	25
<b>6</b>	<b>CAN-Netzwerk</b>	<b>27</b>
6.1	Erstellen oder Ändern eines CAN-Netzwerks	28
<b>7</b>	<b>Ethernet- und CAN-Verbindungs-muster</b>	<b>28</b>
7.1	Zentralennetzwerk über Ethernet	30
7.2	Zentralennetzwerk über CAN	31
7.3	Anschließen von Diensten zur Zentrale	31
7.4	Zentralennetzwerk über Ethernet mit redundanten Zentralen	32
7.5	Zentralennetzwerk über CAN mit redundanten Zentralen	33
7.6	Zentralennetzwerk über zwei Ethernet-Ringe	33
7.7	Zentralennetzwerk über zwei Ethernet-Ringe mit redundanten Zentralen	33
7.8	Ethernet- und CAN-Netzwerk mit redundanten Zentralen verbinden	34
7.9	Remote Services mit redundanten Zentralen verbinden	34
<b>8</b>	<b>Remote Services</b>	<b>35</b>
8.1	Remote Connect	35
8.2	Remote Alert	37
8.3	Remote Maintenance	38
8.4	Remote Portal	40
<b>9</b>	<b>Sprachalarmierungssysteme</b>	<b>43</b>
<b>10</b>	<b>Installation</b>	<b>44</b>
10.1	Einstellungen auf Medienkonvertern	44
10.2	Installieren des Ethernet-Switch	45
10.3	Einstellungen am Switch	45
10.3.1	IP-Adresse vergeben	46
10.3.2	Redundanzeinstellungen programmieren	47
10.3.3	Fehlerrelais programmieren	47
10.3.4	Verbindungsüberwachung programmieren	48
10.3.5	QoS-Priorität, nur bei UGM-2040	48
10.3.6	IGMP Snooping aktivieren	48

---

10.4	CAN-Netzwerk	49
<b>11</b>	<b>Verkabelung</b>	<b>54</b>
11.1	Medienkonverter	55
11.2	Ethernet-Switch	56
11.3	Abgesetzte Bedieneinheit	59
<b>12</b>	<b>FSP-5000-RPS Einstellungen</b>	<b>61</b>
12.1	Netzwerkknotten	61
12.2	Leistungsnummern	61
12.3	Switches	62
12.4	OPC-Server	62
12.5	UGM-2040 Server	63
<b>13</b>	<b>Anhang</b>	<b>64</b>
13.1	Ethernet Fehlermeldungen	64
	<b>Index</b>	<b>66</b>

---



# 1 Sicherheit

In diesem Kapitel finden Sie organisatorische Maßnahmen für PCs, auf denen Service-Clients für das Bosch-Portfolio für Brandmeldetechnik ausgeführt werden. Sie sind verpflichtet, sich an diese vertraglichen Vereinbarungen zu halten.

Sie finden auch nach Themen sortierte Sicherheitshinweise. Später sind die Sicherheitshinweise vor der zugehörigen Anweisung zu finden.

## 1.1 Organisatorische Maßnahmen für Rechner mit Service-Clients

### Einführung

Das Bosch-Portfolio für Brandmeldetechnik umfasst PC-Programme (Service-Clients), die auf einem Rechner laufen und eine physikalische Verbindung zu den Bosch Brandmeldeanlagen erfordern. Aus Sicherheitsgründen und unter Berücksichtigung der gesetzlichen Bestimmungen dürfen Brandmeldeanlagen nicht in einem gemeinsam genutzten Netzwerk installiert werden. Dies wiederum bedeutet, dass das gesamte Netzwerk der Brandmelderzentrale und der Rechner, auf dem ein Service-Client läuft, ein physikalisch dediziertes Netzwerk aufbauen muss. Da Bosch nur die Service-Clients, nicht aber die Computer entwickelt, auf denen sie laufen, können die Rechner nicht von Bosch gesteuert werden. Um das Risiko potenzieller Sicherheitsprobleme zu reduzieren, werden in diesem Dokument organisatorische Maßnahmen definiert.

### Maßnahmen

Wenn die nachfolgend beschriebenen Maßnahmen eine Internetverbindung erfordern, oder der Service-Client zur Lizenzierung eine temporäre Internetverbindung benötigt, muss der Rechner vor der Verbindung mit dem Internet physisch vom Netzwerk der Brandmeldeanlage getrennt werden. Die Internetverbindung muss getrennt werden, bevor der Rechner wieder mit dem Netzwerk der Brandmeldeanlage verbunden wird.

1. Betriebssysteme  
Bosch dokumentiert die Voraussetzungen für die Service-Clients einschließlich der Betriebssystemversionen. Es wird garantiert, dass die Clients mit diesen Versionen kompatibel sind. Das Betriebssystem, auf dem der Client läuft, muss regelmäßig aktualisiert werden, um mögliche Sicherheitsrisiken zu beheben. Das System muss so konfiguriert sein, dass es Schreibzugriff nur auf die Ordner ermöglicht, die für die jeweilige Aufgabe erforderlich sind. Standardmäßig sollen allen Benutzern nur Leserechte erteilt werden.
2. Virenschutz  
Auf den Rechnern muss eine dem aktuellen Stand der Technik entsprechende Virenschutzsoftware installiert und ausgeführt werden. Die Definitionsdateien müssen regelmäßig aktualisiert werden.
3. Firewall  
Auf dem Rechner muss eine Software-Firewall installiert und ausgeführt werden. Sie muss so konfiguriert sein, dass sie den Datenverkehr zwischen dem Service-Client und der Brandmeldeanlage und Updates für das Betriebssystem und die Virenschutzsoftware ermöglicht. Außerdem muss sie den gesamten anderen Datenverkehr blockieren.
4. Sichere Benutzeranmeldung  
Der Zugriff auf den Rechner muss auf Benutzer beschränkt sein, die den installierten Service-Client verwenden. Das Login muss mit dem aktuellen Stand der Technik entsprechenden Mitteln gesichert werden. Wird zur Sicherung des Zugangs ein Passwort gewählt, so müssen die Richtlinien dazu dem neuesten Stand der Technik entsprechen und angewandt werden.

- Die Zwei-Mann-Regel (Vier-Augen-Prinzip) oder die Mehr-Faktor-Authentifizierung sind, falls möglich, empfohlene Ansätze zur Stärkung der Authentifizierung.
5. Software und Dienste  
Der Umfang der auf dem Rechner installierten Software ist auf ein Minimum zu reduzieren. Es sollte nur Software installiert werden, die vom Service-Client und für entsprechende Aufgaben benötigt wird.
  6. Eingeschränkte Nutzung  
Die Nutzung des Rechners ist mit organisatorischen Mitteln auf anwendungsbezogene Aufgaben zu beschränken. Dies gilt auch für die Nutzung des Internets für andere als die in diesem Dokument beschriebenen Zwecke.
  7. Aufgabentrennung  
Aufgaben und Verantwortungsbereiche sollen getrennt werden, um Möglichkeiten für unbefugte oder unbeabsichtigte Änderungen oder Missbrauch zu reduzieren, d.h. unterschiedliche Aufgaben werden unterschiedlichen Rollen zugeordnet.
  8. Überwachung  
Alle Zugriffsversuche auf den Rechner, auf dem der Service-Client läuft, müssen überwacht werden, um unberechtigte Zugriffe auf den Rechner und das Internet zu erkennen.

## 1.2 Erläuterung der Sicherheitssymbole



### **Warnung!**

Weist auf eine gefährliche Situation hin, die, wenn sie nicht vermieden wird, zu schweren Verletzungen oder zum Tod führen kann.



### **Vorsicht!**

Weist auf eine gefährliche Situation hin, die, wenn sie nicht vermieden wird, zu geringen bis mittelschweren Verletzungen führen kann.



### **Hinweis!**

Weist auf eine Situation hin, in der es zu Schäden am Gerät, an der Umgebung oder zu Datenverlust kommen kann, wenn sie nicht vermieden wird.

## 1.3 Sicherheitshinweise

### **Medienkonverter**



### **Warnung!**

Laserlicht

Nicht in den Strahl blicken oder direkt mit optischen Instrumenten (z. B. Lupe, Mikroskop) betrachten. Das Nichtbeachten dieses Hinweises kann Ihre Augen gefährden, wenn der Abstand weniger als 100 mm beträgt. Das Licht tritt an den optischen Anschlüssen oder am Ende der daran angeschlossenen Lichtwellenleiter aus. Diode Klasse 2M, Wellenlänge 650 nm, Leistung < 2 mW, gemäß IEC 60825-1.

---

## Remote Services

---

**Vorsicht!**

Für den Zugang über Internet verwenden Sie nur Bosch Remote Services.

---

**Vorsicht!**

Remote Services erfordert eine sichere IP-Verbindung. Bosch Remote Services oder Verbindung mit Private Secure Network ist erforderlich.

Mit Private Secure Network wird ein IP-Netzwerk auf DSL-Basis mit einem optionalen drahtlosen Zugriff seitens der Zentrale bereitgestellt (EffiLink). Remote Services für Private Secure Network ist in Deutschland nur in Verbindung mit einem Wartungsvertrag für Bosch BT-IE erhältlich.

---

**Hinweis!**

Für den Aufbau eines zentralen Brandmeldenetzes ist ein exklusives Ethernet-Netzwerk notwendig.

Die Verwendung eines Brandmeldesystems in einem anderen Ethernet-Netzwerk erfolgt auf eigenes Risiko des Benutzers. Bosch schließt jegliche Haftung und Gewährleistung für eine falsche Verwendung aus.

Bei Verwendung eines nicht exklusiven Ethernet-Netzwerks kann eine zuverlässige Alarmübertragung und IT-Sicherheit nicht sichergestellt werden.

---

## Zentralennetzwerk

---

**Hinweis!**

EN 54

Verwenden Sie zum EN 54-konformen Aufbau der Netzwerke nur Komponenten, die für den Einsatz in zentralen Brandmeldenetzen zugelassen sind.

Externe RSTP-Switches und Medienkonverter in Ethernet-Netzwerken müssen in Zentralengehäusen montiert werden. Die Montage außerhalb eines Zentralengehäuses ist nicht EN 54-konform.

---

**Hinweis!**

TX-Leitungslänge

Alle IP-Verbindungen müssen direkt oder über Medienkonverter hergestellt werden, die von Bosch genehmigt wurden. Die TX-Leitungslänge von Knoten zu Knoten muss weniger als 100 m betragen.

---

**Hinweis!**

VdS 2540

Um Anforderungen von VdS 2540 an Datenübertragungswege zu erfüllen, verwenden Sie nur Lichtwellenleiter für Ethernet-Verbindungen. Verbindungen innerhalb eines Gehäuses können über Ethernet-Kabel TX hergestellt werden.

---

**Hinweis!**

Verwenden Sie für normale Anwendungen die Standard-Netzwerkeinstellungen.

Änderungen an den Standard-Netzwerkeinstellungen dürfen nur versierte Benutzer mit Netzwerkkennnissen vornehmen.

---

**Hinweis!**

Anwendbare Topologien

Die Funktionalität und Kommunikation der Zentralen untereinander wird durch den Zentralentyp beschränkt. Informationen zu Diensten, die Anzahl der anschließbaren Zentralen und der anschließbaren abgesetzten Bedieneinheiten finden Sie in den technischen Daten der Zentrale.

**2****Einführung**

Dieses Dokument richtet sich an Leser, die Erfahrung in der Planung und Installation von EN 54-konformen Brandmeldesystemen haben. Darüber hinaus sind Netzwerkkennnisse erforderlich.

In diesem Dokument werden eine Reihe von Topologien für Brandmeldenetzwerke beschrieben. Die Topologien werden unabhängig vom Typ der Brandmeldezentrale beschrieben.

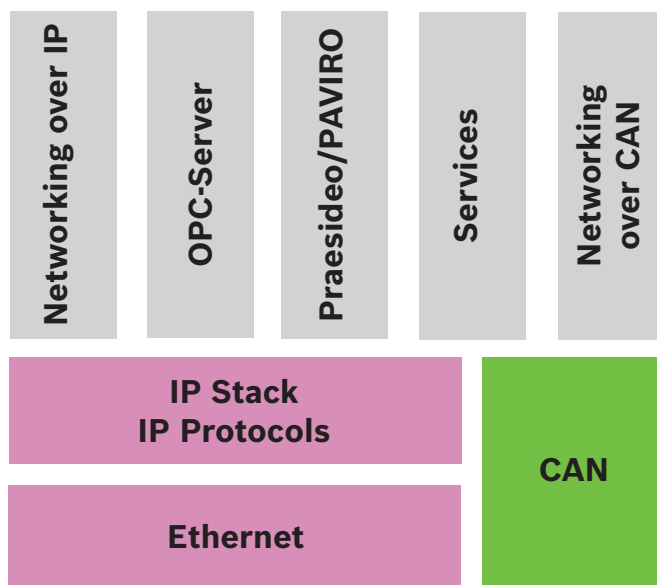
Für den Aufbau von Zentralennetzwerken gemäß den beschriebenen Topologien und um Dienste anzuschließen benötigen Sie die in diesem Dokument beschriebenen Verbindungsmuster.

Das Dokument gibt Ihnen eine Übersicht über die Rahmenbedingungen, Grenzwerte und allgemeinen Vorgehensweisen bei der Planung und Installation.

Detaillierte Beschreibungen der Installation der einzelnen Komponenten finden Sie in den jeweiligen Installationsanleitungen.

Eine Beschreibung der Benutzeroberfläche der Zentralensteuerung finden Sie in der dem Gerät beigelegten Bedienungsanleitung.

Die Benutzeroberfläche der Programmiersoftware FSP-5000-RPS wird in der Onlinehilfe beschrieben.

**3****Systemübersicht**

Im Netzwerk werden die Ethernet-Schnittstelle und IP-Protokolle für unterschiedliche Dienste verwendet. Es ist möglich, entweder die Ethernet-Schnittstelle vollständig zu deaktivieren oder nur die Nutzung für die Vernetzung über TCP/IP zu verhindern. Eine Deaktivierung kann für die Vernetzung über CAN erforderlich sein.

**Bereitstellen von Diensten**

- Vernetzung über TCP/IP

- Aktivieren Sie in FSP-5000-RPS die Kommunikation der Zentralen untereinander im Ethernet-Netzwerk.

  - OPC-Server  
Fügen Sie einen OPC-Server zur FSP-5000-RPS Konfiguration hinzu.
  - Praesideo/PAVIRO-Anschaltung  
Fügen Sie der FSP-5000-RPS Konfiguration ein Sprachalarmierungssystem hinzu und konfigurieren Sie virtuelle Auslöser.
  - Remote Services (Remote Connect als Voraussetzung, Remote Maintenance und Remote Alert)  
Aktivieren Sie das entsprechende Kontrollkästchen in FSP-5000-RPS.
  - Remote Services (Remote Connect als Voraussetzung, Remote Maintenance und Remote Alert) für Private Secure Network  
Fügen Sie der FSP-5000-RPS Konfiguration Fernzugriff hinzu, und richten Sie den Fernzugriff in FSP-5000-RPS ein.

**Hinweis!**



Ungewollte Datenübertragung

Deaktivieren Sie die Kommunikation der Zentrale über TCP/IP in FSP-5000-RPS, wenn die Ethernet-Schnittstelle der Zentralensteuerung nur für die Kommunikation mit einem OPC-Server oder für Remote Services genutzt wird. Andernfalls könnten Branddaten ungewollt über Ethernet übertragen werden.


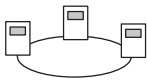

Um Dienste zu betreiben, die auf Ethernet und TCP/IP basieren, müssen die Ethernet-Schnittstellen aktiviert und die TCP/IP-Einstellungen korrekt konfiguriert werden.

**Vernetzung von Zentralen und abgesetzten Bedieneinheiten**

Die folgende Tabelle zeigt die Möglichkeiten der Vernetzung von Zentralen/abgesetzten Bedieneinheiten abhängig von der Topologie und dem Zentralentyp. Beachten Sie die Grenzwerte in Abhängigkeit von der Netzwerktopologie.

Topologie	AVENAR panel 8000, Premium-Lizenz	AVENAR panel 8000, Standard-Lizenz	AVENAR panel 2000, Premium-Lizenz	AVENAR panel 2000, Standard-Lizenz
 Stand-Alone	Möglich	Möglich	Möglich	Möglich
 Ring	Max. 32 Zentralen/ abgesetzte Bedieneinheiten, Verbindung mit AVENAR panel 2000, Premium-Lizenz und FPA	Max. 32 Zentralen/ abgesetzte Bedieneinheiten, Verbindung mit AVENAR panel 2000, Premium-Lizenz und FPA	Max. 32 Zentralen/ abgesetzte Bedieneinheiten, Verbindung mit AVENAR panel 8000 und FPA	1 Zentrale und max. 3 abgesetzte Bedieneinheiten
 Redundanz der Zentrale	Die redundante Zentralensteuerung muss außerdem Premium sein. Sie können auch eine abgesetzte	Die redundante Zentralensteuerung kann Standard sein. Sie können auch eine abgesetzte Bedieneinheit als	Nicht möglich	Nicht möglich

Topologie	AVENAR panel 8000, Premium-Lizenz	AVENAR panel 8000, Standard-Lizenz	AVENAR panel 2000, Premium-Lizenz	AVENAR panel 2000, Standard-Lizenz
	Bedieneinheit als redundante Zentrale verwenden.	redundante Zentrale verwenden.		

Topologie	FPA-5000	FPA-1200
 Stand-Alone	Möglich	Möglich
 Ring	Max. 32 Zentralen und abgesetzte Bedieneinheiten	1 Zentrale und max. 3 abgesetzte Bedieneinheiten
 Redundanz der Zentrale	Möglich	Nicht möglich (DIP 6 an der Zentralensteuerung ist funktionslos).

Wenn Sie ein FPA-5000 Netzwerk erweitern, empfiehlt Bosch, das Netzwerk mit einer Zentrale der AVENAR panel Serie zu erweitern.

Beim Austausch einer Zentrale der FPA Serie durch eine Zentrale der AVENAR panel Serie ist es ausreichend, nur die Zentralensteuerung auszutauschen. Beachten Sie, dass die Zentralen der AVENAR panel Serie keine Adresskarten unterstützen. Falls ein Ethernet-Switch angeschlossen ist, können Sie ihn weiter verwenden.

Prüfen Sie beim Austausch einer abgesetzten Bedieneinheit der FPA Serie durch eine abgesetzte Bedieneinheit der AVENAR panel Serie, ob der Leitungswiderstand im für die Bedieneinheit der AVENAR panel Serie spezifizierten Bereich liegt.

**Hinweis!**



**Firmwareinstallation**

Angeschlossene Zentralen müssen dieselbe Firmwareversion haben.

Eine Firmwareinstallation ist nur für die aktive Zentrale möglich. Führen Sie für redundante Zentralen die Firmwareinstallation für beide Zentralen durch. Hierzu müssen Sie die Rollen der Zentrale wechseln und nach erfolgreicher Firmwareinstallation wieder zurück ändern.



**Hinweis!**

**Redundante Zentralensteuerung**

Es ist nicht möglich, für Redundanzzwecke eine Zentralensteuerung der AVENAR panel Serie mit einer Zentralensteuerung der FPA Serie zu kombinieren.

## 4 Topologien

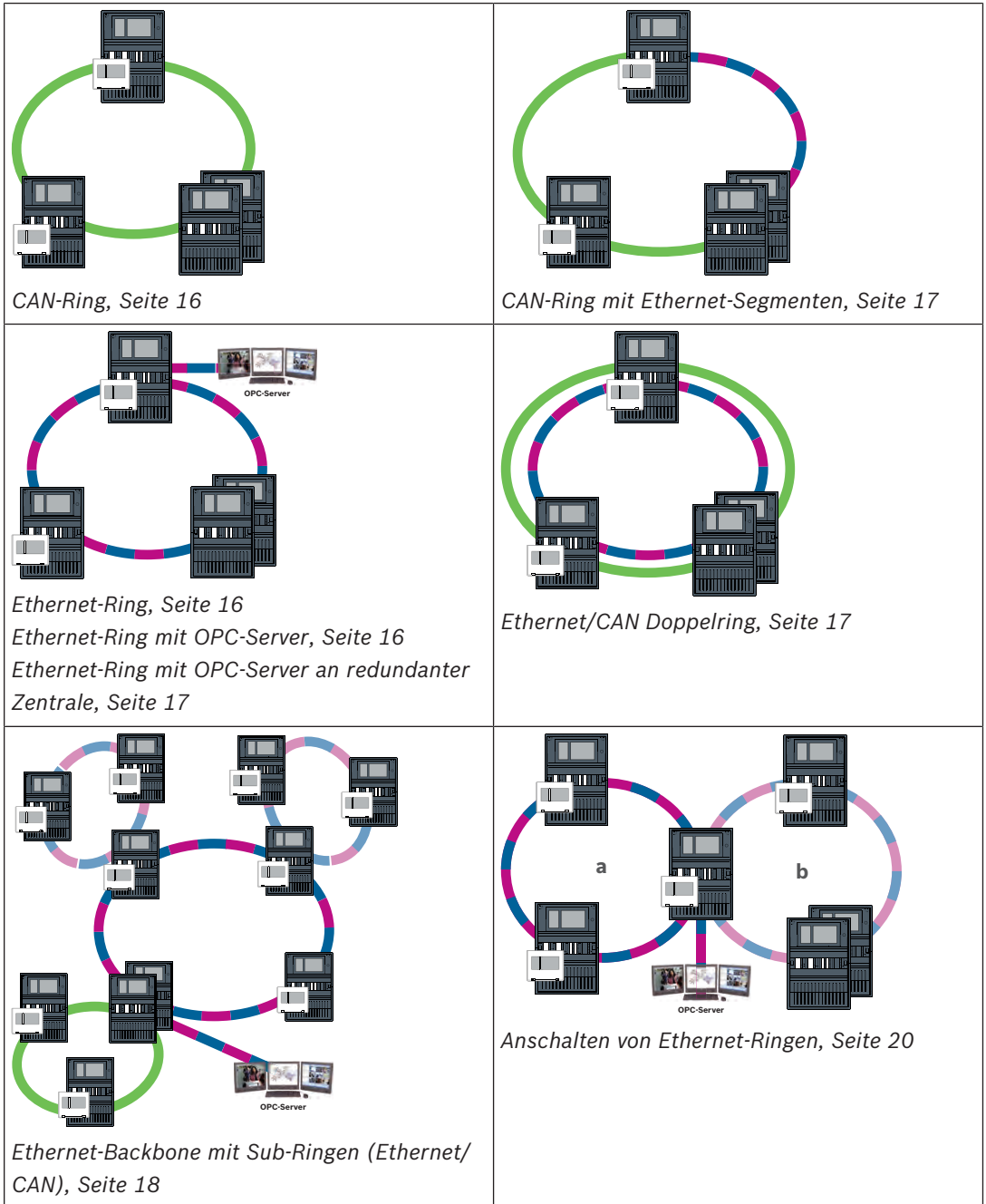
In diesem Dokument werden eine Reihe von Topologien für Brandmeldenetzwerke beschrieben. Die Topologien werden unabhängig vom Typ der Brandmeldezentrale beschrieben.






**Hinweis!**

Anwendbare Topologien

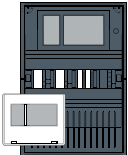

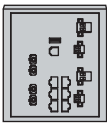


Die Funktionalität und Kommunikation der Zentralen untereinander wird durch den Zentralentyp beschränkt. Informationen zu Diensten, die Anzahl der anschließbaren Zentralen und der anschließbaren abgesetzten Bedieneinheiten finden Sie in den technischen Daten der Zentrale.



Kabel	Beschreibung
	Ethernet-Kabel TX (Kupfer), TX-Leitungslänge Knoten zu Knoten < 100 m

Kabel	Beschreibung
	Ethernet-Kabel FX (Lichtwellenleiter)
	Ethernet-Kabel TX oder FX, TX-Leitungslänge Knoten zu Knoten < 100 m
	CAN-Kabel, CAN-Leitungslänge Knoten zu Knoten < 1000 m

Gerät	Beschreibung
	Zentrale oder abgesetzte Bedieneinheit (in Ethernet-Topologie jeweils ein interner RSTP-Switch)
	Redundante Zentrale (in Ethernet-Topologie interner RSTP-Switch) Eine abgesetzte Bedieneinheit kann als redundante Zentralensteuerung verwendet werden. Die Netzwerkverbindungen und Einstellungen für eine redundante Zentralensteuerung und eine redundante Bedieneinheit sind identisch. Die Verwendung einer redundanten Bedieneinheit gilt nur für AVENAR panel 8000.
	Ethernet-Switch als externer RSTP-Switch (im Allgemeinen Ethernet-Switch MM)
	Medienkonverter
	Sicheres Netzwerk-Gateway für Remote Services

**Grenzwerte im Netzwerk**

Die Anzahl der vernetzbaren Zentralen bzw. abgesetzten Bedieneinheiten hängt von der Wahl der Netzwerktopologie ab.

Bei Vernetzung werden Zentralen und abgesetzte Bedieneinheiten als Knoten bezeichnet.

- Die Anzahl der Meldepunkte in einem Netzwerk ist auf 32768 beschränkt.
- Die Anzahl der Meldepunkte pro Zentrale, die in einem Netzwerk betrieben wird, ist auf 2048 beschränkt.
- Die Anzahl der Knoten pro Anlage ist abhängig von der Art der Topologie.  
Ein Knoten ist entweder eine Zentralensteuerung oder eine abgesetzte Bedieneinheit.
- Die Anzahl der Knoten in der Ringtopologie ist auf 32 beschränkt.
- Mit FSP-5000-RPS können einer Zentrale bis zu 3 konfigurierte abgesetzte Bedieneinheiten zugewiesen werden.

Die Verkabelung zwischen den Knoten und die zulässige Leitungslänge sind ebenfalls von der gewählten Topologie abhängig.

Es können bis zu 32 Zentralensteuerungen, Abgesetzte Bedieneinheiten und OPC-Server zu einem Netzwerk zusammengeschlossen werden.

Je nach Verwendungszweck können verschiedene Zentralensteuerungen und Abgesetzte Bedieneinheiten in Gruppen eingeteilt, als Netzwerkknoten oder lokale Knoten definiert werden. In der Regel können innerhalb einer Gruppe lediglich Zustände der Zentralen



angezeigt werden, die sich ebenfalls innerhalb der definierten Gruppe befinden. Von Netzwerkknoten aus können Zustände aller Zentralen unabhängig von der Gruppenzugehörigkeit angezeigt bzw. bearbeitet werden.

#### **Physikalische Knotenadresse**

Eine Zentrale oder abgesetzte Bedieneinheit wird im Netzwerk durch eine eindeutige Adresse identifiziert, die als physikalische Knotenadresse bezeichnet wird.



#### **Hinweis!**

Physikalische Knotenadresse für redundante Zentralen

Eine redundante Zentrale muss dieselbe physikalische Knotenadresse wie die zugeordnete primäre Zentrale haben.



#### **Hinweis!**

Das verwendete Netzwerk muss mindestens folgende Voraussetzungen erfüllen:

Mindestdurchsatz: 1 Mbps

Maximale Latenz: 250 ms



#### **Hinweis!**

EN 54

Verwenden Sie zum EN 54-konformen Aufbau der Netzwerke nur Komponenten, die für den Einsatz in zentralen Brandmeldernetzwerken zugelassen sind.

Externe RSTP-Switches und Medienkonverter in Ethernet-Netzwerken müssen in Zentralengehäusen montiert werden. Die Montage außerhalb eines Zentralengehäuses ist nicht EN 54-konform.



#### **Hinweis!**

Redundante Zentrale – EN 54-2

Pro Zentrale dürfen gemäß EN 54-2 maximal 512 Meldepunkte angeschlossen werden. Wenn diese Anzahl überschritten wird, muss die Zentrale redundant ausgeführt werden.

Wenn eine Zentrale als Schnittstelle mit einem CAN-Sub-Ring fungiert und mehr als 512 Meldepunkte im Sub-Ring angeschlossen sind, muss die Zentrale redundant ausgeführt werden. Die Redundanz wird über den RSTP-Switch erreicht, der 2 Ringe verbindet.

Für eine Stand-Alone-Zentrale können bis zu 4096 Meldepunkte angeschlossen werden, auch wenn sie redundant ausgeführt wird. Wenn die Zentrale Teil eines Netzwerks ist, können Sie maximal 2048 Meldepunkte anschließen.



#### **Hinweis!**

Achten Sie darauf, dass die der Zentrale zugewiesene physikalische Knotenadresse mit der in der Programmiersoftware identisch ist. Letztere ist für die Einstellung der letzten Zahl der IP-Adresse in den Standardeinstellungen verantwortlich.

Aktivieren Sie RSTP als Redundanzprotokoll und übernehmen Sie die Standardwerte.

#### **Standard-Ethernet-Einstellungen der Brandmeldezentrale**

In den Standardeinstellungen der Brandmelderzentrale übernimmt sowohl die Programmiersoftware FSP-5000-RPS als auch die Bedieneinheit die festgelegte physikalische Knotenadresse als letzte Zahl der IP-Adresse.



#### **Hinweis!**

Voraussetzung für ein lauffähiges Netzwerk ist die korrekte Einstellung der physikalischen Knotenadresse an der Zentralensteuerung und in der Programmiersoftware FSP-5000-RPS.

**Hinweis!**

Die Verwendung der Ethernet-Redundanz muss in der Zentralensteuerung separat angesteuert werden.

- IP-Einstellungen
  - IP-Adresse 192.168.1.x  
Die letzte Zahl der IP-Adresse ist in den Standardeinstellungen immer mit der an der Zentralensteuerung eingestellten physikalischen Knotenadresse identisch.
  - Netzmaske 255.255.255.0
  - Gateway 192.168.1.254
  - Multicast-Adresse 239.192.0.1
  - Port-Nummer 25001 – 25008 (nur der erste Port kann festgelegt werden, es werden immer 8 aufeinander folgende Ports verwendet)
- RSTP-Parameter (Standardeinstellungen)
  - Bridge Priority 32768
  - Hello Time 2
  - Max. Age 20
  - Forward Delay 15

**Hinweis!**

Sie können die Standardeinstellungen der IP-Konfiguration mit Netzwerken bis zu 20 RSTP-Switches verwenden.

Bei Netzwerken mit mehr als 20 RSTP-Switches sind topologieabhängig zusätzliche Einstellungen erforderlich. Vertieftes Netzwerkwissen ist dafür erforderlich.

**Einstellungen für Ringe mit mehr als 20 RSTP-Switches**

Wenn es im Netzwerk mehr als 20 RSTP-Switches gibt, müssen Sie die RSTP-Einstellungen an der Zentralensteuerung und in der Programmiersoftware anpassen. Zentralensteuerungen, abgesetzte Bedieneinheiten und die angeschlossenen externen RSTP-Switches gelten als RSTP-Switches. Redundante Zentralensteuerungen gelten nicht als RSTP-Switches, da der darin enthaltene Switch nicht als RSTP-Switch betrieben wird.

- RSTP-Parameter
  - Lassen Sie Bridge Priority bei 32768
  - Lassen Sie Hello Time bei 2
  - Ändern Sie Max. Age von 20 zu 40
  - Ändern Sie Forward Delay von 15 zu 25

**Parameter**

- Es können maximal 32 Knoten in einem Ring verwendet werden.
- Der Durchmesser des Netzwerks darf nicht größer sein als 32 (siehe *Netzwerkdurchmesser, Seite 22*).
- Ethernet-Switches dürfen nicht außerhalb des Zentralengehäuses verwendet werden.
- Medienkonverter dürfen nicht außerhalb des Zentralengehäuses verwendet werden.

**Leistungsmerkmale**

- Das Netzwerk ist EN 54-konform.
- Das Netzwerk verwendet RSTP.

### Verbindung von BIS mit OPC-Server

Bei Anschluss an ein Gebäudemanagementsystem (BIS) über einen OPC-Server und Ethernet 100BaseTX innerhalb gebäudeübergreifender Netzwerke muss mit dem Netzwerkverantwortlichen geklärt werden, ob:

1. das Netzwerk für gebäudeübergreifende Verbindungen ausgelegt ist (z. B. keine technische Beeinflussung durch Potenzialunterschiede in der Erdverbindung)
2. die Bandbreite der Teilnehmer für das Netzwerk ausreichend ist

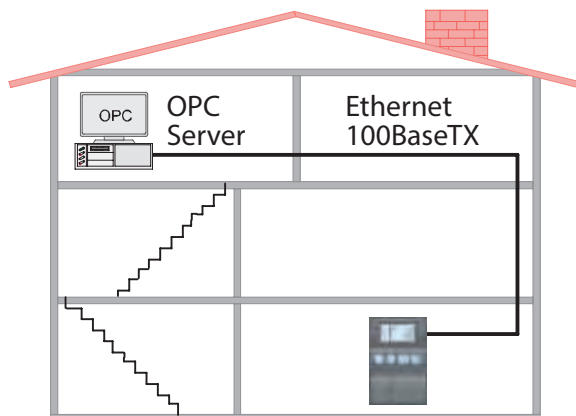


Abbildung 4.1: Anbindung an BIS über einen OPC-Server

### Weitere Informationen für die Verwendung eines OPC-Servers

OPC-Server in Ihrem Netzwerk müssen zur Programmiersoftware FSP-5000-RPS hinzugefügt werden.

Sie müssen die folgenden Einstellungen in der Software FSP-5000-RPS und beim OPC-Server festlegen:

- Netzwerkknoten
- Netzwerkgruppe
- RSN
- IP-Adresse
- Port

Der OPC-Server verwendet standardmäßig den Port 25000.

#### Hinweis!

EN 54

Die Verbindung eines Gebäudemanagementsystems (z. B. BIS) über eine Ethernet-Schnittstelle mit einem OPC-Server oder FSI-Server ist EN 54-konform, wenn die EN 54-relevanten Funktionen nur von der Brandmelderzentrale ausgeführt werden. Alle EN 54-relevanten Steuerungs- oder Verwaltungsfunktionen (z. B. Steuerung von Signalgebern oder Abschaltungsverwaltung) mit dem Gebäudemanagementsystem erfordern, dass eine individuelle EN 54-Zertifizierung des gesamten Systems von einem Zertifizierungsinstitut vorliegt.



#### Hinweis!

Programmiersoftware FSP-5000-RPS

Sie müssen jedem Netzwerkknoten einen OPC-Server zuweisen, von dem Status übertragen werden soll.



## 4.1

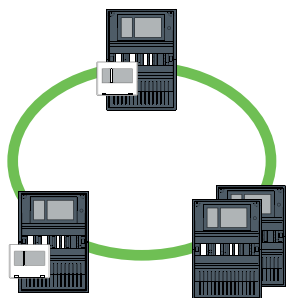
**CAN-Ring**

Abbildung 4.2: CAN-Ring

## 4.2

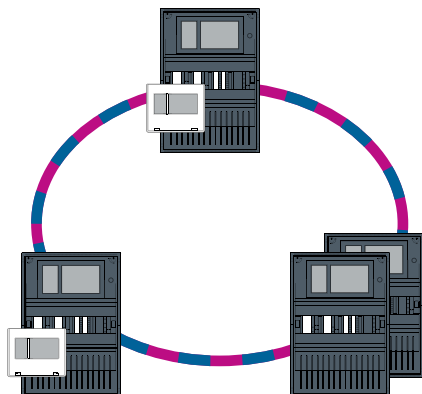
**Ethernet-Ring**

Abbildung 4.3: Ethernet-Ring

## 4.3

**Ethernet-Ring mit OPC-Server****Ethernet-Switch zur Anschaltung des OPC-Servers muss separat programmiert werden**

Programmieren Sie die IP-Adresse und die Redundanzeinstellungen des Ethernet-Switch (siehe *Einstellungen am Switch, Seite 45*). Da der Switch in unmittelbarer Nähe (ohne Zwischenraum) installiert ist, muss die Stromversorgung nicht redundant ausgeführt werden, und die Störungsausgänge werden dementsprechend nicht genutzt.

Achten Sie darauf, dass die RSTP-Einstellungen in den Zentralensteuerungen, in FSP-5000-RPS und im Ethernet-Switch gleich sind.

**OPC-Server muss separat programmiert werden**

Programmieren Sie die IP-Adresse, Netzwerkknoten, Netzwerkgruppe und die RSN. Weitere Informationen finden Sie im entsprechenden Abschnitt des Kapitels zur Installation im Handbuch Vernetzung.

Der OPC-Server verwendet standardmäßig den Port 25000.

Stellen Sie sicher, dass die Einstellungen in der Programmiersoftware FSP-5000-RPS und im OPC-Server identisch sind.

**Parameter**

- Der OPC-Server kann über ein Ethernet-Kabel (Kupfer) oder einen Lichtwellenleiter angeschlossen werden.

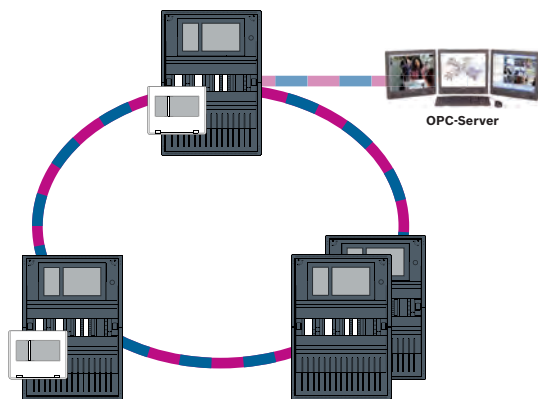


Abbildung 4.4: Ethernet-Ring mit OPC-Server

#### 4.4 Ethernet-Ring mit OPC-Server an redundanter Zentrale

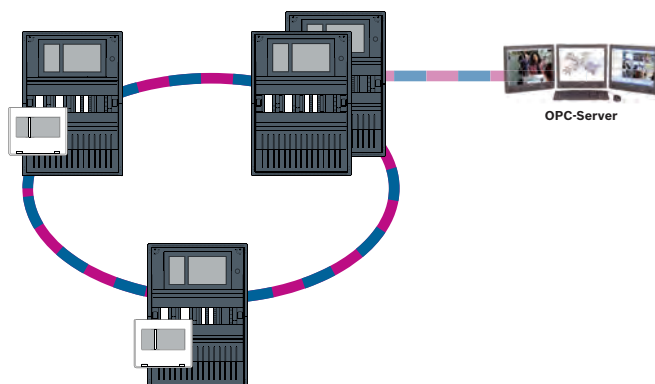


Abbildung 4.5: Ethernet-Ring mit OPC-Server an redundanter Zentrale

#### 4.5 Ethernet/CAN Doppelring

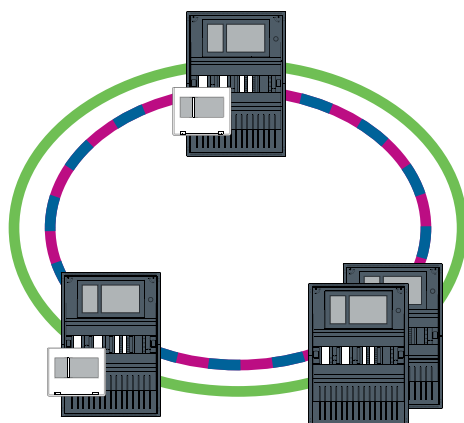


Abbildung 4.6: Doppelter Ring von Ethernet und CAN

#### 4.6 CAN-Ring mit Ethernet-Segmenten

Die Haupttopologie ist ein CAN-Ring. Wenn der Abstand zwischen zwei Knoten mehr als 1000 m beträgt, kann zur Überbrückung eine FX-Ethernet-Verbindung verwendet werden.

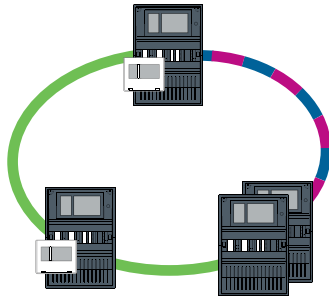


Abbildung 4.7: CAN-Ring mit Ethernet-Segmenten

## 4.7

### Ethernet-Backbone mit Sub-Ringen (Ethernet/CAN)

Ein Ethernet-Backbone ist an alle Sub-Ringe angeschlossen. Daher handelt es sich um einen wichtigen Verbindungsbereich mit hohen Datenübertragungsraten. Die RSTP-Switches im Backbone sind standardmäßig nicht übergeordnet. Beachten Sie, dass Sie bei dieser Topologie den Netzwerkdurchmesser bestimmen müssen. Zentralensteuerungen, abgesetzte Bedieneinheiten und die angeschlossenen externen RSTP-Switches gelten als RSTP-Switches. Über CAN-Netzwerk vernetzte Zentralen werden beim Bestimmen des Netzwerkdurchmessers ignoriert.

Beachten Sie die Einstellungen für Ringe mit mehr als 20 RSTP-Switches (siehe *Einstellungen für Ringe mit mehr als 20 RSTP-Switches*, Seite 14).



#### Hinweis!

Diese Topologie erfordert zusätzliche Einstellungen für alle RSTP-Switches im Backbone. Daher ist vertieftes Netzwerkwissen erforderlich.



#### Hinweis!

Stellt die Zentrale eine Schnittstelle an einen CAN-Subring dar, so muss diese Zentrale nach EN 54-2 auch dann redundant ausgeführt werden, wenn im Subring mehr als 512 Meldepunkte angeschlossen sind.

In einem Ethernet-Subring gilt diese Einschränkung nicht, da die Switches zur Verbindung der beiden Ringe die Redundanz übernehmen.

#### Optionale Einstellungen

Sie müssen den zentralen Ring als Backbone betreiben. Dieser zentrale Ring muss über Ethernet vernetzt werden.



#### Hinweis!

Legen Sie für alle RSTP-Switches im Backbone eine höhere RSTP-Priorität als in den Sub-Ringen fest. Dadurch wird sichergestellt, dass die RSTP-Root-Bridge selbst bei einer Störung immer im Backbone bleibt.

Die RSTP-Switches zum Verbinden der Ringe sind Teil des Backbone!

Verwenden Sie eine RSTP-Priorität von 16384 im Backbone.



#### Hinweis!

Je niedriger der festgelegte Wert, desto höher die RSTP-Priorität.

### Switches für den Anschluss des OPC-Servers und der Sub-Ringe müssen separat programmiert werden

Programmieren Sie die IP-Adresse und die Redundanzeinstellungen der Ethernet-Switches (siehe *Einstellungen am Switch, Seite 45*). Für diese Topologie müssen die Störungsausgänge nur verwendet werden, wenn Sie die Stromversorgung des Switch redundant ausgeführt haben oder eine Verbindung von Switch zu Switch besteht (siehe *Ethernet-Switch, Seite 56*). Achten Sie darauf, dass die RSTP-Einstellungen in den Zentralensteuerungen, in FSP-5000-RPS und im Ethernet-Switch gleich sind.



#### Hinweis!

Ändern Sie die RSTP-Priorität für die RSTP-Switches, die die Ringe verbinden, da sie zum Backbone gehören.

### Der OPC-Server muss separat programmiert werden.

Programmieren Sie die IP-Adresse, Netzknoten, Netzgruppe und RSN, siehe *OPC-Server, Seite 62*.

Der OPC-Server verwendet standardmäßig den Port 25000.

Achten Sie darauf, dass die Einstellungen in der Programmiersoftware RPS und im OPC-Server gleich sind.

#### Parameter

- Der OPC-Server kann über ein Ethernet-Kabel (Kupfer) oder einen Lichtwellenleiter angeschlossen werden.

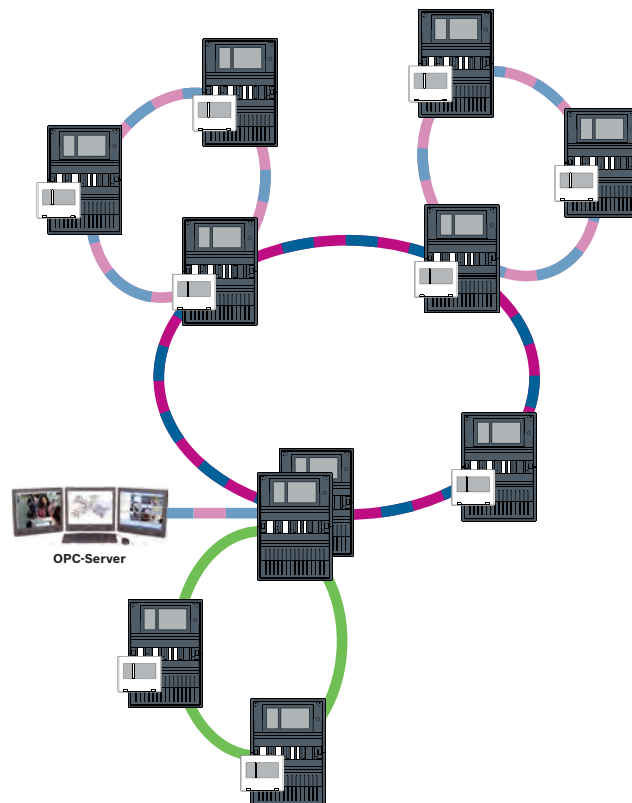


Abbildung 4.8: Ethernet-Backbone mit Sub-Ringen

## 4.8 Anschalten von Ethernet-Ringen



### Hinweis!

Diese Topologie erfordert zusätzliche Einstellungen für alle RSTP-Switches im Backbone. Daher ist vertieftes Netzwerkwissen erforderlich.

### Optionale Einstellungen

Diese Topologie ist eine spezielle Instanz des Ethernet-Backbone mit Sub-Ringen (siehe Ethernet-Backbone mit Sub-Ringen (Ethernet/CAN)). Sie müssen einen der zwei Ringe als Backbone ausführen.



### Hinweis!

Legen Sie für alle Zentralen und Switches im Backbone eine höhere RSTP-Priorität als in den Sub-Ringen fest. Dadurch wird sichergestellt, dass die RSTP-Root-Bridge selbst bei einer Störung immer im Backbone bleibt.

Die Switches zum Verbinden der zwei Ringe sind Teil des Backbone!

Verwenden Sie eine RSTP-Priorität von 16384 im Backbone.



### Hinweis!

Je niedriger der festgelegte Wert, desto höher die RSTP-Priorität.

### Switches für den Anschluss des OPC-Servers und des zweiten Rings müssen separat programmiert werden

Programmieren Sie die IP-Adresse und die Redundanzeinstellungen des Ethernet-Switch (siehe *Einstellungen am Switch, Seite 45*). Für diese Topologie müssen die Störungsausgänge nur verwendet werden, wenn Sie die Stromversorgung des Switch redundant ausgeführt haben (siehe *Ethernet-Switch, Seite 56*).

Achten Sie darauf, dass die RSTP-Einstellungen in den Zentralensteuerungen, in FSP-5000-RPS und im Ethernet-Switch gleich sind.

Ändern Sie die RSTP-Priorität für die Switches zum Verbinden der zwei Ringe, da sie zum Backbone gehören.

### OPC-Server muss separat programmiert werden

Programmieren Sie die IP-Adresse, Netzwerkknoten, Netzwerkgruppe und die RSN. Weitere Informationen finden Sie im entsprechenden Abschnitt des Kapitels zur Installation im Handbuch Vernetzung.

Der OPC-Server verwendet standardmäßig den Port 25000.

Stellen Sie sicher, dass die Einstellungen in der Programmiersoftware FSP-5000-RPS und im OPC-Server identisch sind.

### Parameter

- Der OPC-Server kann über ein Ethernet-Kabel (Kupfer) oder einen Lichtwellenleiter angeschlossen werden.

In diesen Beispielen ist Ring a der Backbone. Ring b ist der Sub-Ring.



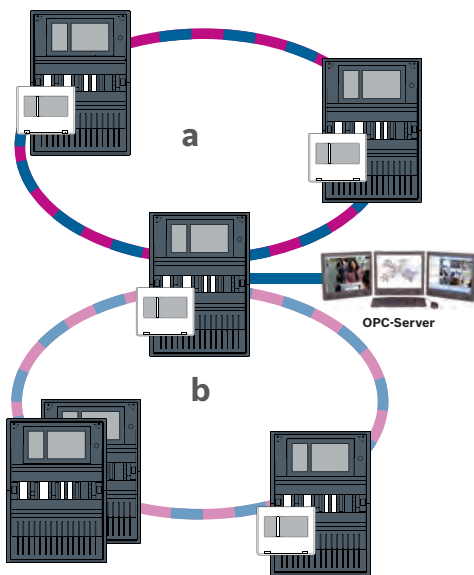


Abbildung 4.9: Anschalten des Ethernet-Rings über eine nicht redundante Zentrale

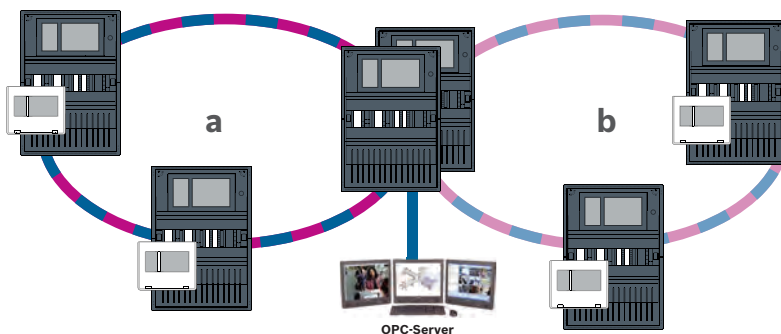


Abbildung 4.10: Anschalten des Ethernet-Rings über eine redundante Zentrale

## 5 Ethernet-Netzwerk

Im Netzwerk werden die Ethernet-Netzwerkverbindungen kontinuierlich überwacht. Wenn eine Verbindung getrennt ist, wird diese Unterbrechung erkannt. Reparierte Verbindungen werden ebenfalls erkannt. Die Netzwerkdiagnose der Zentrale zeigt Ihnen immer die MAC-Adresse der Hosts an, die über das Netzwerk verbunden sind.

### MAC-Adressen

Für den Netzwerkanschluss bietet jede Zentralensteuerung die folgenden MAC-Adressen.

- MAC-Adresse für den Host
- MAC-Adresse zum Identifizieren des ETH1-Ports
- MAC-Adresse zum Identifizieren des ETH2-Ports

Abhängig vom Zentralensteuerungstyp:

- MAC-Adresse zum Identifizieren des ETH3-Ports
- MAC-Adresse zum Identifizieren des ETH4-Ports

### Regeln für die Verwendung von vier Ethernet-Ports

Wenn Ihre Zentrale über vier Ethernet-Ports verfügt, wenden Sie die folgenden Regeln in der angegebenen Reihenfolge an. Bosch unterstützt ausschließlich Netzwerke, die gemäß den folgenden Regeln aufgebaut wurden.

1. Für die Zentralenvernetzung müssen Sie ETH1 und ETH2 verwenden. Ein externer RSTP-Switch auf ETH1 oder ETH2 darf nur für die Zentralenvernetzung verwendet werden.

2. Für die Anschaltung von OPC, FSM-5000-FSI, Praesideo/PAVIRO und UGM-2040 müssen Sie ETH3 verwenden. Sie können einen externen RSTP-Switch verbinden, der nicht für die Zentralenvernetzung verwendet werden darf.
3. Für Remote Services müssen Sie ETH4 verwenden. Wenn keine Verbindung zu Remote Services erforderlich ist, kann ETH4 für die Anschaltung von OPC, FSM-5000-FSI, Praesideo/PAVIRO oder UGM-2040 eingesetzt werden.
4. Wenn keine Zentralenvernetzung über ETH1 und ETH2 existiert, können beide für die Anschaltung von OPC, FSM-5000-FSI, Praesideo/PAVIRO oder UGM-2040 verwendet werden.

## 5.1 Protokolle

### SNMP

SNMP wird zur Überwachung und Kontrolle von Netzwerkknoten verwendet. Hier können Parameter von Netzwerkknoten gelesen oder geändert werden. Dafür benötigen Sie eine entsprechende Netzwerkverwaltungssoftware (z. B. Hirschmann HiVision).



#### Hinweis!

Das Netzwerk verwendet die feste SNMP-Community-Zeichenfolge: PUBLIC

Beachten Sie, dass die AVENAR panel Serie noch nicht das SNMP-Protokoll unterstützt.

### LLDP

LLDP ist ein einfaches, von dem IEEE standardisiertes Protokoll, mit dem Netzwerk-Informationen zwischen benachbarten Geräten ausgetauscht werden. Diese Informationen werden

- als Teil der SNMP-Daten zur Verfügung gestellt und
- als Teil der Netzwerk-Diagnosedaten über die Zentralensteuerung angezeigt.

### RSTP

RSTP ist ein von IEEE vereinheitlichtes Netzwerkprotokoll. RSTP stellt die Schleifenfreiheit in Netzwerken sicher. Redundante Pfade werden im Netzwerk erkannt, deaktiviert und im Bedarfsfall aktiviert (Ausfall einer Verbindung).

Das Protokoll wird für genau diesen Zweck im Netzwerk verwendet.

Eine Änderung der Topologie nach einem Verbindungsausfall wird nach deren Reparatur automatisch zurückgenommen.

## 5.2 Netzwerkdurchmesser

Der Netzwerkdurchmesser des RSTP-Ethernet-Zentralennetzwerks darf nicht größer als 32 sein.



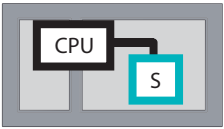
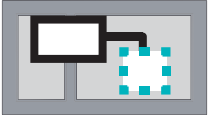
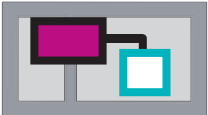
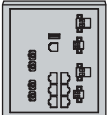
### Definition

Der Durchmesser eines Netzwerks entspricht der Anzahl der RSTP-Switches auf dem längst möglichen Abschnitt ohne Ringe zwischen zwei beliebigen Endpunkten im Netzwerk.

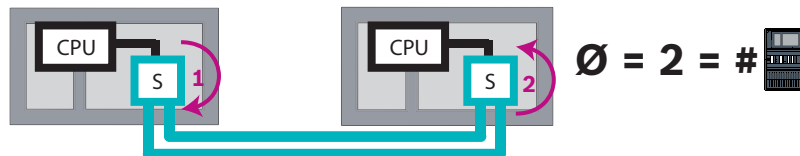
Folgendes muss in Bezug auf ein RSTP-Ethernet-Zentralennetzwerk berücksichtigt werden:

- Jede Zentralensteuerung enthält einen Endpunkt und einen internen RSTP-Switch.
- Eine Kombination aus Zentralensteuerung und redundanter Zentralensteuerung zählt als nur ein RSTP-Switch.
- Medienkonverter gelten nicht als RSTP-Switches.
- CAN-Verbindungen können nicht in den längst möglichen Abschnitt aufgenommen werden.
- OPC-Server werden bezüglich des Durchmessers nicht berücksichtigt.

**Schlüssel**

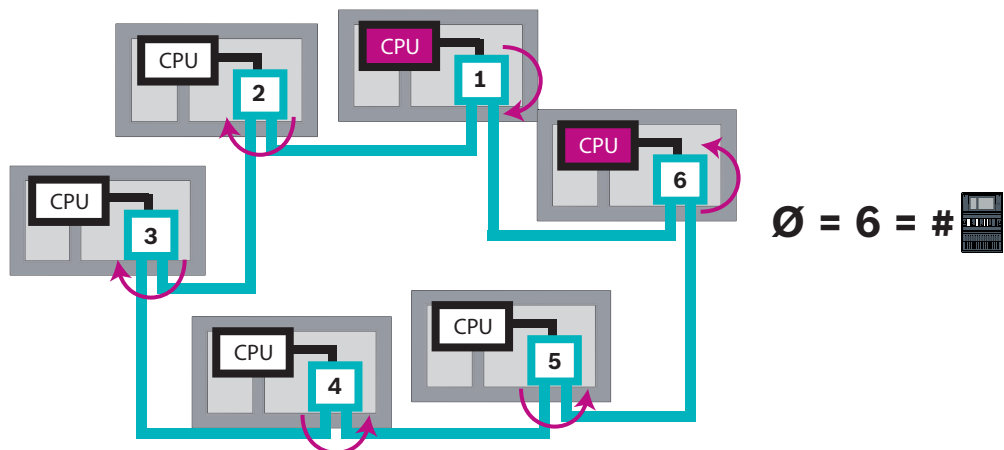
	Zentraler Prozessor in der Zentralensteuerung oder in der abgesetzten Bedieneinheit.
	Interner RSTP-Switch in der Zentralensteuerung oder im abgesetzten Bedienfeld.
	Zentralensteuerung oder abgesetztes Bedienfeld mit zentralem Prozessor und internem RSTP-Switch.
	Redundante Zentralensteuerung mit zentralem Prozessor und internem RSTP-Switch.
	Zentralensteuerung oder abgesetzte Bedieneinheit Start- oder Endpunkt für das Bestimmen des Netzwerkdurchmessers in den Beispielen.
	Ethernet-Switch als externer RSTP-Switch (im Allgemeinen Ethernet-Switch MM)

Zwei angeschlossene Zentralen bilden den kleinstmöglichen Ring. Der Durchmesser dieses Netzwerks entspricht 2, da sich die internen RSTP-Switches zwischen den Endpunkten befinden.



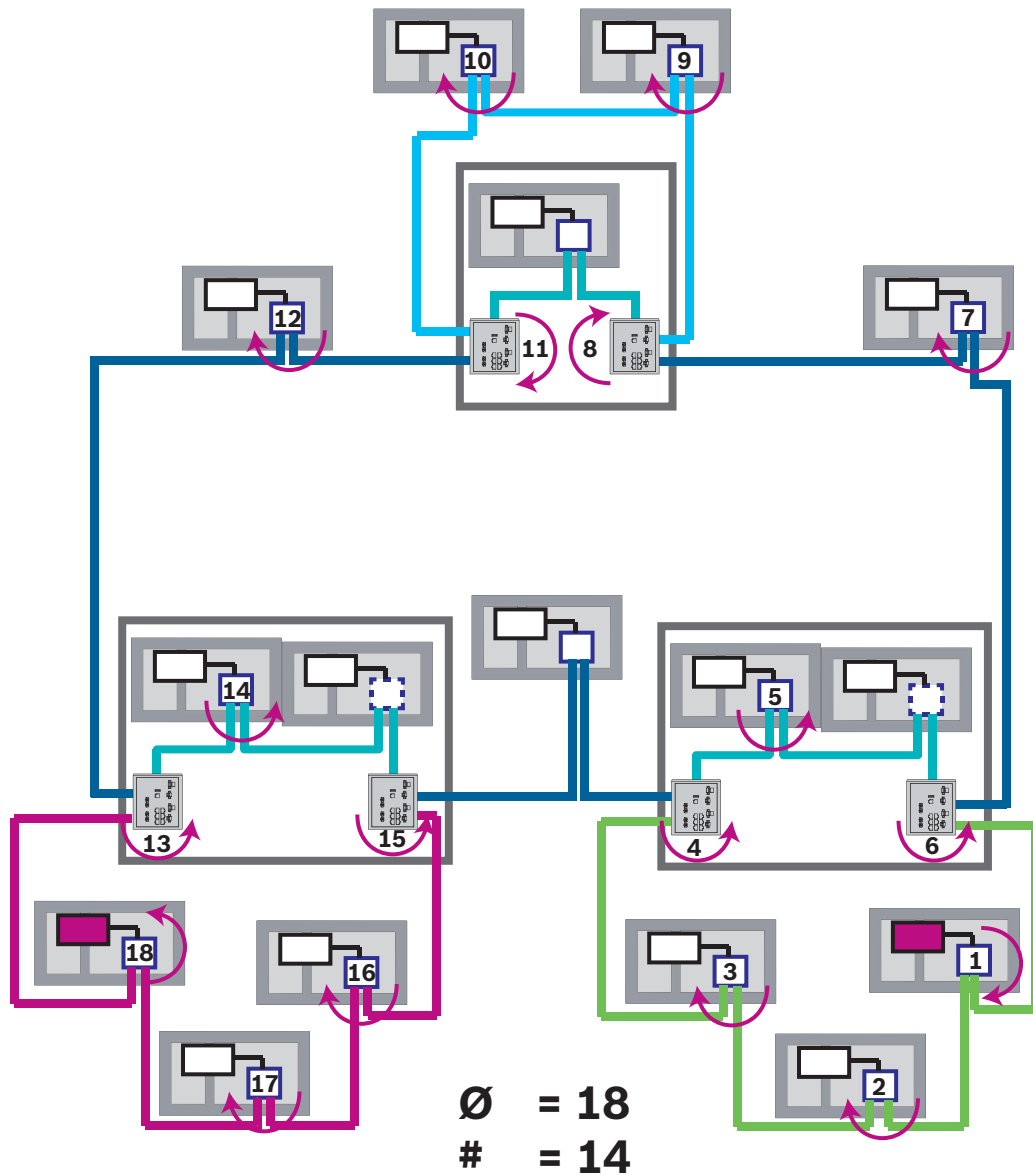
**Abbildung 5.1: Netzwerkdurchmesser eines Rings mit zwei Zentralen**

In einem Zentralenring ohne externe RSTP-Switches entspricht der Durchmesser des Netzwerks der Anzahl der installierten Zentralen.



**Abbildung 5.2: Netzwerkdurchmesser eines Rings mit sechs Zentralen**

Wenn ein Backbone und Sub-Ringe über Ethernet-Switches miteinander verbunden sind, müssen diese externen RSTP-Switches auch berücksichtigt werden.



**Abbildung 5.3: Netzwerkdurchmesser eines Backbones mit Sub-Ringen**

Die Abbildung zeigt, dass für den Durchmesser der längste Pfad gefunden werden muss.

## 5.3

### Verwendete Kabel

Verwenden Sie für die Vernetzung nur folgende Kabel. Die Verwendung von anderen Kabeln entspricht nicht den Sicherheitsstandards in den EU-Richtlinien.

- Ethernet-Kabel  
Ethernet-Patchkabel, geschirmt, CAT 5e oder besser.  
Beachten Sie die in der Kabelspezifikation angegebenen minimalen Biegeradien.
- Lichtwellenleiter  
Multimode: Lichtwellenleiter-Ethernet-Patchkabel, Duplex I-VH2G 50/125 $\mu$  oder Duplex I-VH2G 62.5/125 $\mu$ , SC-Stecker.  
Single mode: Lichtwellenleiter-Ethernet-Patchkabel, Duplex I-VH2E 9/125 $\mu$ , SC-Stecker.  
Beachten Sie die in der Kabelspezifikation angegebenen minimalen Biegeradien.

**Hinweis!****TX-Leitungslänge**

Alle IP-Verbindungen müssen direkt oder über Medienkonverter hergestellt werden, die von Bosch genehmigt wurden. Die TX-Leitungslänge von Knoten zu Knoten muss weniger als 100 m betragen.

**Hinweis!****VdS 2540**

Um Anforderungen von VdS 2540 an Datenübertragungswege zu erfüllen, verwenden Sie nur Lichtwellenleiter für Ethernet-Verbindungen. Verbindungen innerhalb eines Gehäuses können über Ethernet-Kabel TX hergestellt werden.

## 5.4

### Erstellen oder Ändern eines Ethernet-Netzwerks

Es gibt verschiedene Verfahren zur Erstellung eines Ethernet-Netzwerks von Brandmelderzentralen. Die beiden unten beschriebenen Verfahren unterscheiden sich in der Größe der Netzwerke und der Anzahl der Installationen und Konfigurationsaufgaben, die nebeneinander ausgeführt werden.

**Regeln für die Verwendung von vier Ethernet-Ports**

Wenn Ihre Zentrale über vier Ethernet-Ports verfügt, wenden Sie die folgenden Regeln in der angegebenen Reihenfolge an. Bosch unterstützt ausschließlich Netzwerke, die gemäß den folgenden Regeln aufgebaut wurden.

1. Für die Zentralenvernetzung müssen Sie ETH1 und ETH2 verwenden. Ein externer RSTP-Switch auf ETH1 oder ETH2 darf nur für die Zentralenvernetzung verwendet werden.
2. Für die Anschaltung von OPC, FSM-5000-FSI, Praesideo/PAVIRO und UGM-2040 müssen Sie ETH3 verwenden. Sie können einen externen RSTP-Switch verbinden, der nicht für die Zentralenvernetzung verwendet werden darf.
3. Für Remote Services müssen Sie ETH4 verwenden. Wenn keine Verbindung zu Remote Services erforderlich ist, kann ETH4 für die Anschaltung von OPC, FSM-5000-FSI, Praesideo/PAVIRO oder UGM-2040 eingesetzt werden.
4. Wenn keine Zentralenvernetzung über ETH1 und ETH2 existiert, können beide für die Anschaltung von OPC, FSM-5000-FSI, Praesideo/PAVIRO oder UGM-2040 verwendet werden.

**Erstellen eines Ethernet-Netzwerks (kleinere Projekte)**

Dieses Vorgehen ist für Projekte geeignet, bei denen nur wenige Techniker gleichzeitig an der Installation des Brandmeldesystems arbeiten.

1. Planen Sie das Netzwerk.
2. Erstellen Sie das Netzwerk in FSP-5000-RPS und konfigurieren Sie die Netzwerkeinstellungen.
3. Drucken Sie die Netzwerkinformationen zur Aufbewahrung aus oder speichern Sie die Informationen auf dem Laptop.
4. Installieren Sie die Zentralen und Netzwerkabel und verbinden Sie diese zu einem Netzwerk.
5. Konfigurieren Sie die Netzwerkeinstellungen der einzelnen Zentralen direkt an der Bedieneinheit gemäß Ausdruck.
6. Setzen Sie jede der Zentralen im Netzwerk zurück, um die Netzwerkkonfiguration zu aktivieren.

7. Verbinden Sie Ihren Computer mithilfe der FSP-5000-RPS Programmiersoftware mit einer Zentrale im Netzwerk. Laden Sie die Konfiguration über diese Zentrale auf alle anderen Zentralen im Netzwerk. Redundante Zentralen verwenden die Konfiguration der Hauptzentrale.
8. Führen Sie eine Rücksetzung durch, um die anstehenden Fehlermeldungen zurückzusetzen. Beheben Sie alle Fehler.

Konfigurieren Sie zunächst die Netzwerkeinstellungen auf den Zentralen. Dadurch haben Sie den Vorteil, dass Sie die anderen Zentralen im Netzwerk von einer Zentrale aus programmieren können.

### **Erstellen eines Ethernet-Netzwerks (mittelgroße und große Projekte)**

Dieses Vorgehen ist für Projekte geeignet, bei denen mehrere Aufgaben gleichzeitig von mehreren Teams ausgeführt werden. Da viele Aufgaben während der Installation und Konfiguration den Neustart der Brandmelderzentrale erfordern, wird das Netzwerk bei diesem Vorgehen erst zu einem späteren Zeitpunkt gestartet.

1. Planen Sie das Netzwerk.
2. Erzeugen Sie eine Konfiguration des Netzwerks ohne Peripheriegeräte mithilfe von FSP-5000-RPS.
3. Drucken Sie die Netzwerkinformationen zur Aufbewahrung aus oder speichern Sie die Informationen auf dem Laptop.
4. Installieren Sie die Netzwerkkabel und überprüfen Sie einzelne Abschnitte oder Ringe.
5. Installieren Sie die Zentralen und nehmen Sie sie als Standalone-Zentralen in Betrieb.
6. Installieren Sie die Peripheriegeräte an den Zentralen.
7. Konfigurieren Sie jede der Zentralen mit FSP-5000-RPS.
8. Stellen Sie sicher, dass die einzelnen Zentralen ordnungsgemäß funktionieren.
9. Nehmen Sie die einzelnen Ringe des Netzwerks nacheinander und gemäß der Topologie in Betrieb.

Beginnen Sie mit dem Backbone.

- Erzeugen Sie eine Konfiguration für den Backbone mit FSP-5000-RPS. Importieren Sie alle erforderlichen Zentralenkonfigurationen. Konfigurieren Sie die Netzwerkeinstellungen, und drucken Sie sie aus.
- Verbinden Sie alle Zentralen zu einem Netzwerk.
- Konfigurieren Sie die Netzwerkeinstellungen der einzelnen Zentralen direkt an der Zentralensteuerung gemäß Ausdruck.
- Setzen Sie jede der Zentralen zurück, um die Netzwerkkonfiguration zu laden.
- Pingen Sie die benachbarten Zentralen an, um das Netzwerk zu überprüfen.
- Nehmen Sie den gesamten Backbone in Betrieb und beheben Sie alle Fehler.

Nehmen Sie die Sub-Ringe entsprechend dem Backbone-Beispiel in Betrieb.

### **Hinzufügen einer Zentrale zu einem Netzwerk**

1. Ändern Sie die Netzwerkkonfiguration in FSP-5000-RPS.
2. Drucken Sie die Netzwerkinformationen zur Aufbewahrung aus oder speichern Sie die Informationen auf dem Laptop.
3. Installieren Sie die Zentrale und Netzwerkkabel und verbinden Sie diese mit dem Netzwerk.
4. Konfigurieren Sie die Netzwerkeinstellungen der individuellen Zentrale direkt an der Bedieneinheit gemäß Ausdruck.
5. Setzen Sie die Zentrale und angrenzenden Zentralen zurück, um die Netzwerkkonfiguration zu aktivieren.

### **Entfernen einer Zentrale aus dem Netzwerk**

1. Ändern Sie die Netzwerkkonfiguration in FSP-5000-RPS.

2. Drucken Sie die Netzwerkinformationen zur Aufbewahrung aus oder speichern Sie die Informationen auf dem Laptop.
3. Konfigurieren Sie die Netzwerkeinstellungen der angrenzenden Zentralen direkt an der Bedieneinheit gemäß Ausdruck.
4. Schalten Sie die Zentrale und die Stromversorgung (Netzteil und Batterie) aus, bevor Sie sie aus dem Netzwerk entfernen.
5. Setzen Sie die angrenzenden Zentralen zurück, um die Netzwerkkonfiguration zu aktivieren.

## 6 CAN-Netzwerk

### Ringtopologie

In der Ringtopologie wird das CAN-Kabel immer von einem CAN1-Terminal zu einem CAN2-Terminal geführt [CAN1 ⇒ CAN2]. Die Kabellänge hängt vom Kabelquerschnitt ab.

### CAN-Verbindung

Die CAN-Verbindung erfolgt zweidrig (CAN-H und CAN-L). Verbinden Sie CAN-H mit CAN-H und CAN-L mit CAN-L für eine zweidrigte Verbindung. In Ausnahmefällen, z. B. bei hoher EMV-Belastung oder einem großen Unterschied im Erdpotential, kann eine dreidrigte Verbindung (CAN-H, CAN-L und CAN-GND) notwendig sein. Verbinden Sie CAN-H mit CAN-H, CAN-L mit CAN-L und CAN-GND mit CAN-GND für eine dreidrigte Verbindung. Der Schirmbeidraht des CAN-Kabels wird nur auf einer Seite mit dem Metallgehäuse der Zentrale verbunden.

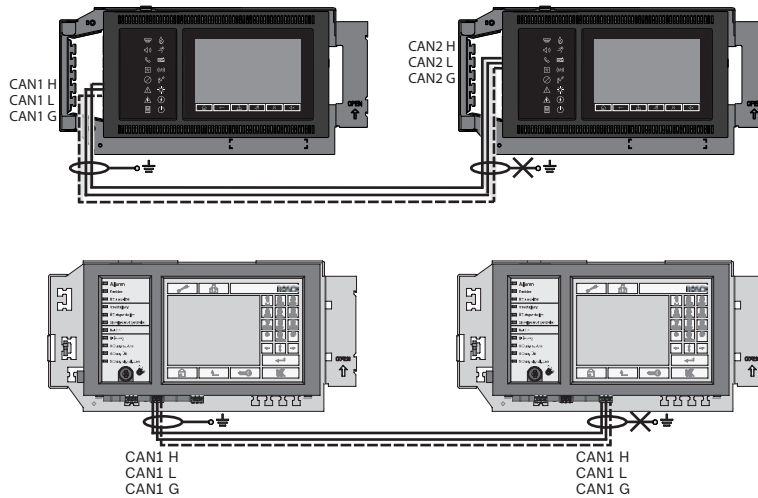


Abbildung 6.1: CAN-Verbindung (oben: AVENAR, unten: FPA)

### Leitungslänge für Vernetzung

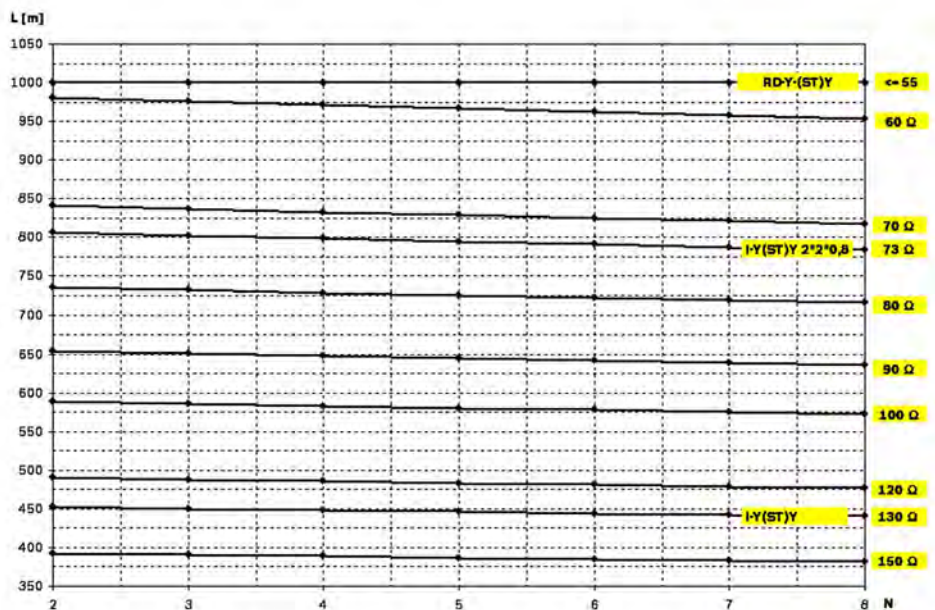
Die maximal zulässige Leitungslänge ist abhängig vom Schleifenwiderstand des verwendeten Kabels und von der Anzahl der kommunizierenden Knoten.

Beispiel: Mit dem Brandmeldekabel J-Y (St) Y 2 x 2 x 0,8 mm, rot, können zwei Knoten mit einer maximalen Distanz von ca. 800 m verbunden werden.



### Hinweis!

Den Abstand zweier Knoten bei Ringtopologie ermitteln Sie, indem Sie den Wert bei zwei Knoten im Diagramm ablesen.



**Abbildung 6.2: CAN-Netzwerk: Erreichbare Leitungslänge abhängig von der Anzahl der Knoten und dem Leitungswiderstand**

L = Leitungslänge in Meter

N = Anzahl Knoten

## 6.1 Erstellen oder Ändern eines CAN-Netzwerks

Dieses Vorgehen ist für Projekte geeignet, bei denen nur wenige Techniker gleichzeitig an der Installation des Brandmeldesystems arbeiten.






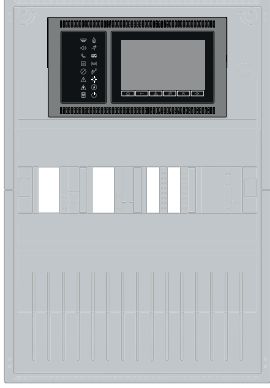
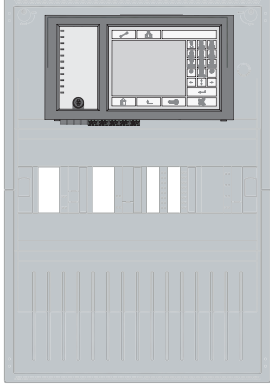
### Vorgehen zum Erstellen eines CAN-Netzwerks

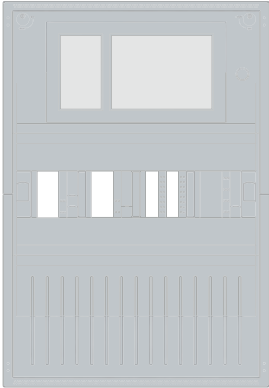
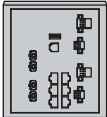



1. Planen Sie das Netzwerk.
2. Erstellen Sie das Netzwerk in FSP-5000-RPS.
3. Drucken Sie die Netzwerkinformationen zur Aufbewahrung aus oder speichern Sie die Informationen auf dem Laptop.
4. Installieren Sie die Zentralen und verbinden Sie sie mit CAN-Kabel zu einem Netzwerk.
5. Verbinden Sie Ihren Computer mithilfe der FSP-5000-RPS Programmiersoftware mit einer Zentrale im Netzwerk. Laden Sie die Konfiguration über diese Zentrale auf alle anderen Zentralen im Netzwerk. Redundante Zentralen verwenden die Konfiguration der Hauptzentrale.
6. Führen Sie eine Rücksetzung durch, um die anstehenden Fehlermeldungen zurückzusetzen. Beheben Sie alle Fehler.

## 7 Ethernet- und CAN-Verbindungsmuster

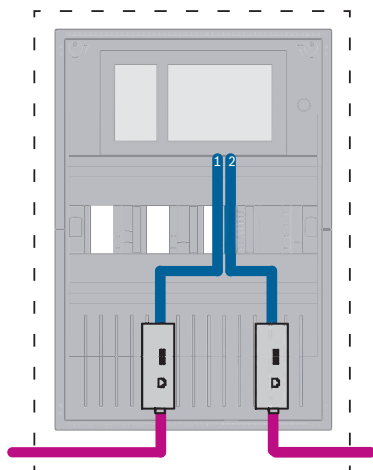
Für den Aufbau von Zentralennetzwerken gemäß den beschriebenen Topologien und um Dienste anzuschließen benötigen Sie die in diesem Dokument beschriebenen Verbindungsmuster.



Symbol	Beschreibung
	Ethernet-Kabel TX (Kupfer), TX-Leitungslänge Knoten zu Knoten < 100 m
	Ethernet-Kabel FX (Lichtwellenleiter)
	Ethernet-Kabel TX oder FX, TX-Leitungslänge Knoten zu Knoten < 100 m
	CAN-Kabel
	Gehäuse Hinweis: Um die Übersicht der verschiedenen Netzwerkmuster zu erleichtern, zeigen die Abbildungen in diesem Kapitel zum Symbolisieren einer Zentrale immer ein kleines Zentralengehäuse. Dieses kleine Gehäuse bietet <b>nicht</b> in allen beschriebenen Fällen ausreichend Platz für die Montage der dargestellten Switches, Medienkonverter und Gateways. Verwenden Sie Safety Systems Designer, um sicherzustellen, dass Sie die korrekte Gehäuseanzahl und -größe für die Montage der Ausrüstung bestellen.
	AVENAR panel
	FPA

Symbol	Beschreibung
	AVENAR panel oder FPA
	Ethernet-Switch als externer RSTP-Switch (im Allgemeinen Ethernet-Switch MM)
	Medienkonverter
	Sicheres Netzwerk-Gateway für Remote Services
	Anbindung an OPC-Server, FSM-5000-FSI, Praesideo/PAVIRO oder UGM-2040

## 7.1 Zentralennetzwerk über Ethernet



**Abbildung 7.1: Zentralennetzwerk über Ethernet**

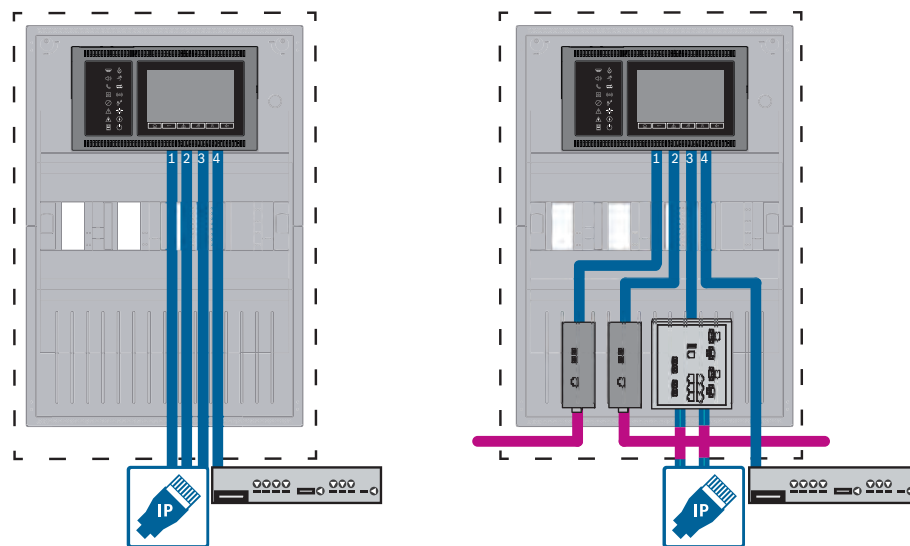
Für Bereiche größer als 100 m ist die Bereichserweiterung mit Medienkonvertern vorgeschrieben. Für Bereiche kleiner als 100 m sind Medienkonverter möglicherweise nicht erforderlich.

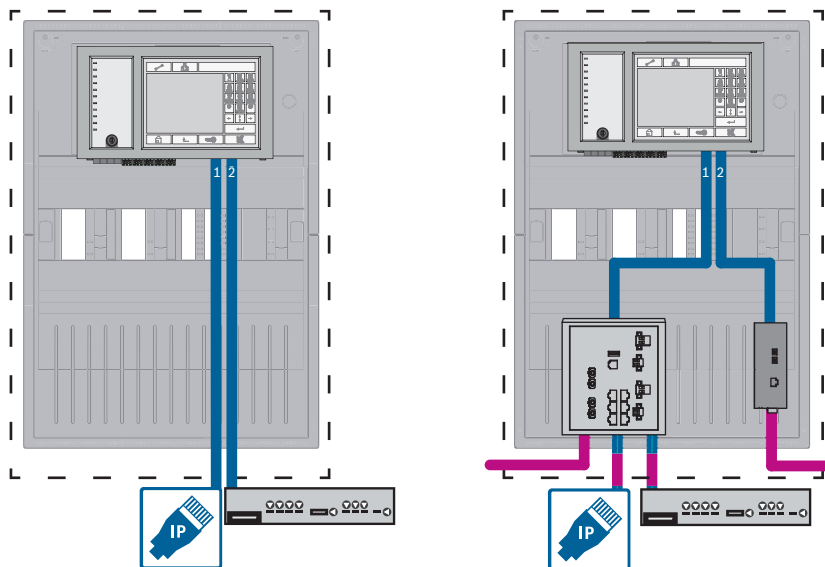
## 7.2 Zentralennetzwerk über CAN



Abbildung 7.2: Zentralennetzwerk über CAN

## 7.3 Anschließen von Diensten zur Zentrale

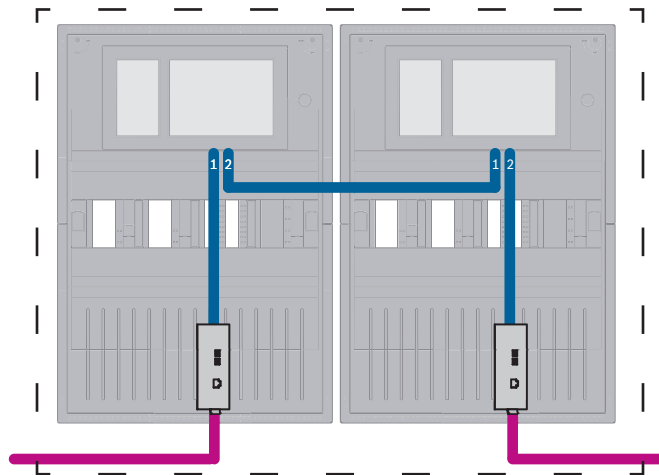




**Abbildung 7.3:** Links: ohne Zentralnetzwerk, rechts: mit Zentralnetzwerk

Für Bereiche größer als 100 m ist die Bereichserweiterung mit Medienkonvertern vorgeschrieben. Für Bereiche kleiner als 100 m sind Medienkonverter möglicherweise nicht erforderlich.

## 7.4 Zentralnetzwerk über Ethernet mit redundanten Zentralen



**Abbildung 7.4:** Zentralnetzwerk über Ethernet mit redundanten Zentralen

Für Bereiche größer als 100 m ist die Bereichserweiterung mit Medienkonvertern vorgeschrieben. Für Bereiche kleiner als 100 m sind Medienkonverter möglicherweise nicht erforderlich.

### 7.5 Zentralennetzwerk über CAN mit redundanten Zentralen

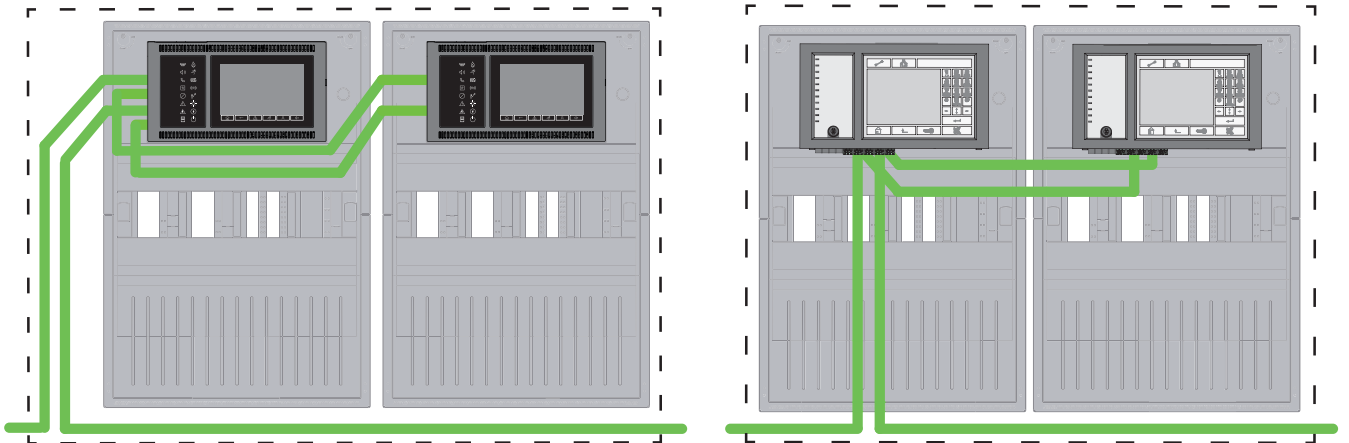


Abbildung 7.5: Zentralennetzwerk über CAN mit redundanten Zentralen

### 7.6 Zentralennetzwerk über zwei Ethernet-Ringe

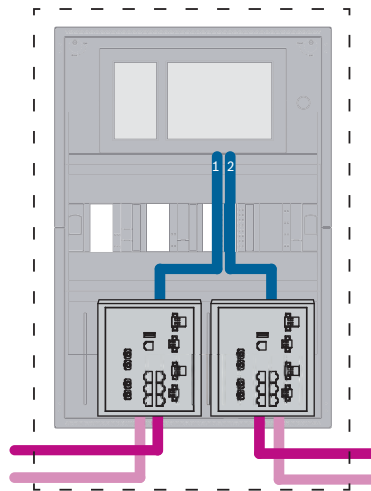


Abbildung 7.6: Ethernet-Netzwerke verbinden

### 7.7 Zentralennetzwerk über zwei Ethernet-Ringe mit redundanten Zentralen

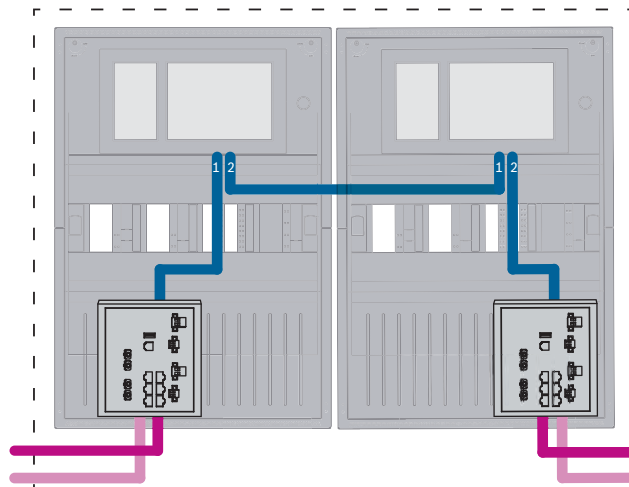


Abbildung 7.7: Ethernet-Netzwerke mit redundanten Zentralen verbinden

## 7.8 Ethernet- und CAN-Netzwerk mit redundanten Zentralen verbinden

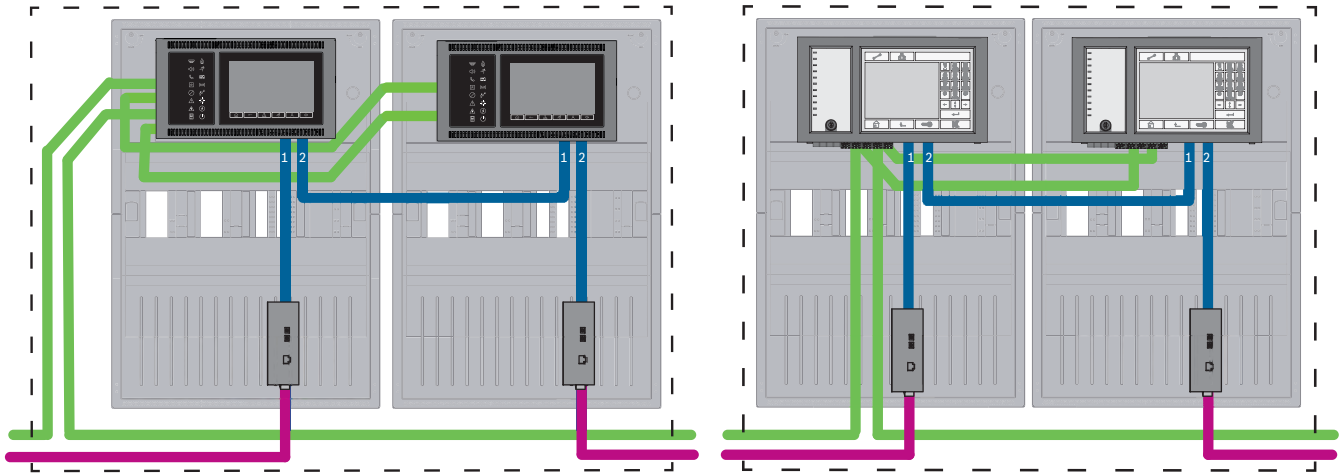
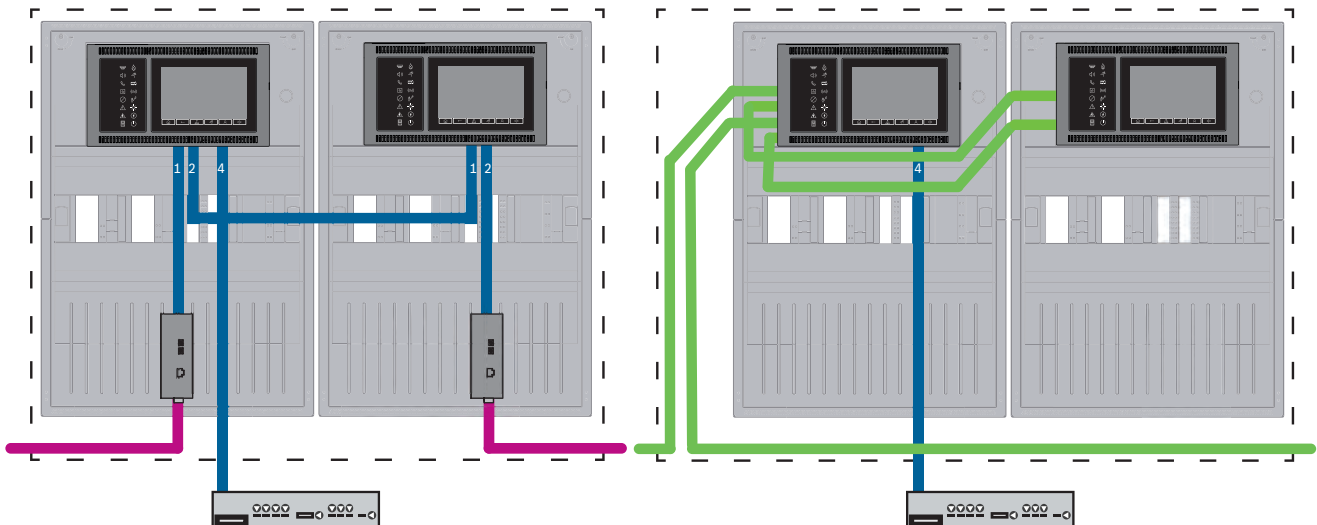


Abbildung 7.8: Ethernet- und CAN-Netzwerk mit redundanten Zentralen verbinden

Für Bereiche größer als 100 m ist die Bereichserweiterung mit Medienkonvertern vorgeschrieben. Für Bereiche kleiner als 100 m sind Medienkonverter möglicherweise nicht erforderlich.

## 7.9 Remote Services mit redundanten Zentralen verbinden



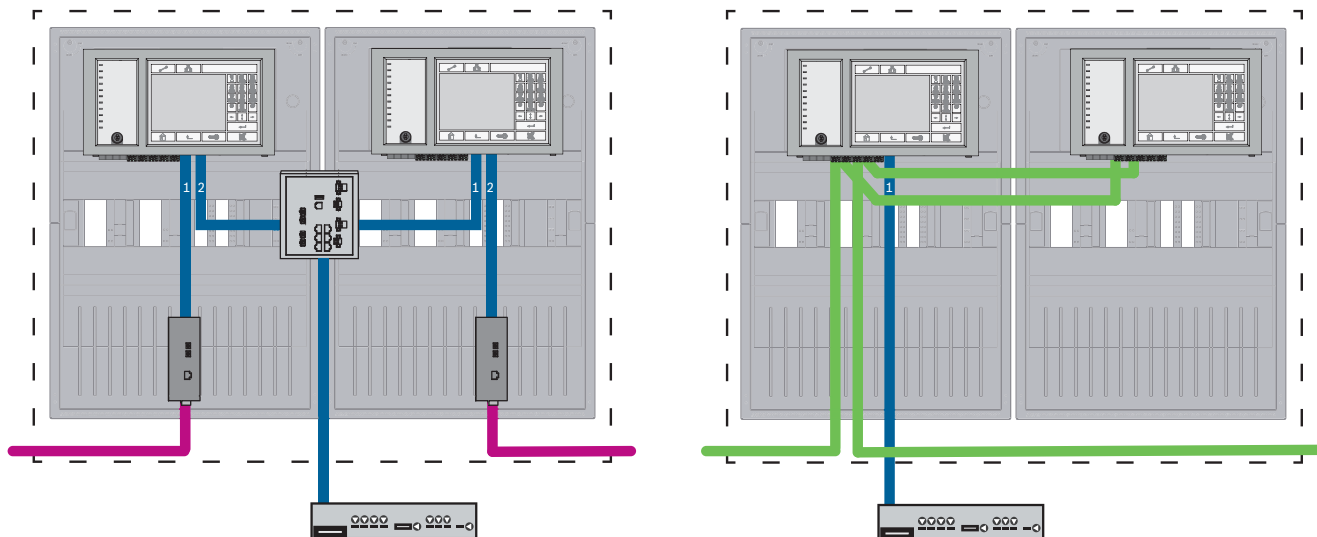


Abbildung 7.9: Links: im Ethernet-Netzwerk Rechts: im CAN-Netzwerk

Für Bereiche größer als 100 m ist die Bereichserweiterung mit Medienkonvertern vorgeschrieben. Für Bereiche kleiner als 100 m sind Medienkonverter möglicherweise nicht erforderlich.

## 8 Remote Services

Die folgenden Dienste gehören zu Remote Services:

- Remote Connect
- Remote Alert
- Remote Maintenance

Voraussetzung für Remote Alert und Remote Maintenance ist Remote Connect.

### 8.1 Remote Connect

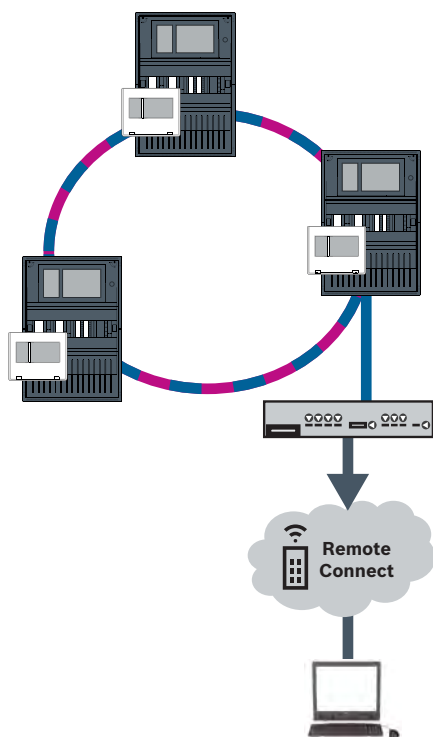
Remote Connect sorgt für eine zuverlässige und sichere Internetverbindung, die den Fernzugriff auf eine Zentrale über FSP-5000-RPS herstellt. Remote Connect ist die Grundlage für alle Remote Services. Verwenden Sie für Remote Connect das sichere Netzwerk-Gateway. Bei Zentralennetzwerken muss eine Zentrale des Zentralennetzwerks mit einem sicheren Netzwerk-Gateway verbunden sein. Ausschließlich diese Verbindung muss eine dedizierte Ethernet-Verbindung sein.



#### Hinweis!

Während Remote Connect die Verbindung zu einem Zentralennetzwerk über Ethernet oder CAN unterstützt, wird die Funktionalität von Remote Alert und Remote Maintenance nur dann unterstützt, wenn eine Ethernet-Vernetzung zwischen Zentralen existiert und für die Verwendung des Diensts konfiguriert ist.

Remote Connect muss in der FSP-5000-RPS Konfiguration dieser Zentrale aktiviert sein. Die folgende Topologie zeigt Zentralensteuerungen, die über Ethernet verbunden sind, wobei ein sicheres Netzwerk-Gateway mit dem Netzwerk über einen Ethernet-Switch (im Allgemeinen MM) verbunden ist.



**Abbildung 8.1: Remote Connect in einem Ethernet-Ring**



**Hinweis!**

Um Zentralen über FX zu verbinden, verwenden Sie von Bosch zugelassene Medienkonverter.

Um zu verhindern, dass EN 54-2-relevanter Multicast-Verkehr an den Router gesendet wird, verwenden Sie den Ethernet-Switch (im Allgemeinen MM, BPA-ESWEX-RSR20), freigegeben mit Zentralenversion 2.8. Aktivieren Sie IGMP-Snooping des Ethernet-Switch. Weitere Informationen finden Sie im entsprechenden Abschnitt des Kapitels zur Installation im Handbuch Vernetzung.



**Hinweis!**

Der Internetrouter (oder das Unternehmensnetzwerk, das den Internetzugang zur Verfügung stellt) wie auch das sichere Netzwerk-Gateway müssen separate Sub-Netzwerke zur Verfügung stellen. Zentralen im Zentralennetzwerk können nicht im Sub-Netzwerk des Internetrouters platziert werden. Auch ein Überlappen der Sub-Netzwerke ist nicht möglich. Bei überlappenden Sub-Netzwerken müssen Sie die Sub-Netzwerke trennen, indem Sie die IP-Adresse seitens der Zentralennetzwerke ändern.

Zudem müssen Sie die Änderungen an das sichere Netzwerk-Gateway weitergeben. Um dies zu tun, müssen Sie die Web-Anwendung über einen Internetbrowser starten.

- Adresse: <https://192.168.1.254>

- Benutzername: bosch

- Passwort: ipti83

Unter **Configuration -> Network (LAN)** können Sie die IP-Adresse ändern. Denken Sie daran, dass die **Standard-Gateway**-Adresse in der Zentralensteuerungskonfiguration die gleiche IP-Adresse haben muss wie das sichere Netzwerk-Gateway.

**Hinweis!**

Gemäß DIBt-Richtlinie ist es nicht erlaubt über Remote Services eine Fernrückstellung zur Wiederherstellung der Funktionsbereitschaft für Feststellanlagen mit motorischer Öffnungshilfe durchzuführen.

Die folgende Topologie zeigt ein CAN-Netzwerk, bei dem ein sicheres Netzwerk-Gateway mit dem Netzwerk über einen Ethernetport verbunden ist.

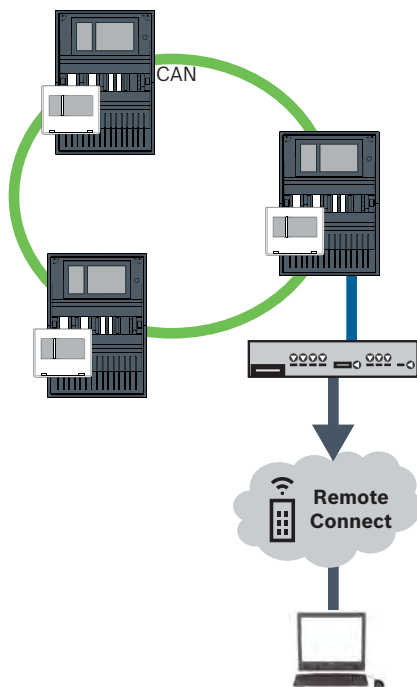


Abbildung 8.2: Remote Connect in einem CAN-Ring

## 8.2

### Remote Alert

Über Remote Alert versorgt eine Zentrale das Remote Portal mit relevanten Statusinformationen.

Übertragene Daten werden mit Remote Alert analysiert. Bei einem unerwarteten Ereignis wird der Benutzer per SMS und/oder E-Mail über den Erhalt von Alarmmeldungen benachrichtigt.

Remote Alert ist auch für Private Secure Network verfügbar.

## 8.3 Remote Maintenance

Remote Maintenance bietet die Möglichkeit der Fernüberwachung bestimmter Parameter verschiedener Elemente, die mit einer Brandmelderzentrale verbunden sind. Über das Remote Portal können Sie Revisionen durchführen.

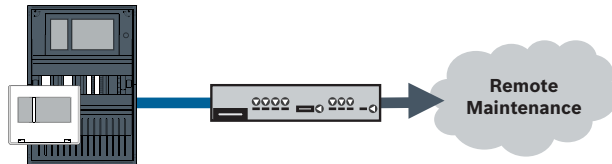


Abbildung 8.3: Remote Maintenance



### Hinweis!

Ethernet-Verbindungen, die nur zur Datenübertragung für Remote Maintenance verwendet werden, können als Ethernet-Kabel oder als Lichtwellenleiter ausgeführt werden. Beachten Sie die maximal zulässigen Leitungslängen.



### Hinweis!

Um Zentralen über FX zu verbinden, verwenden Sie von Bosch zugelassene Medienkonverter.

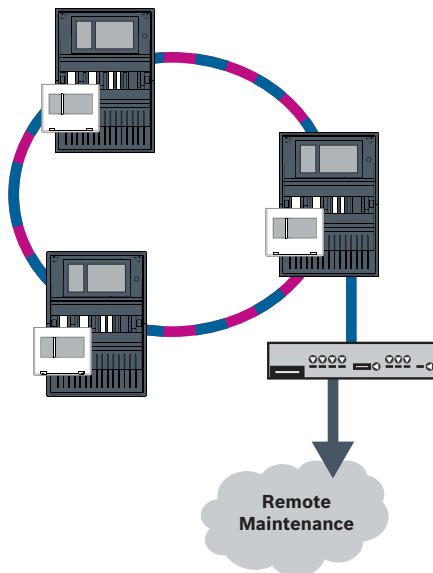


Abbildung 8.4: Remote Maintenance

Bei der Verwendung von Remote Maintenance mit Ethernet-Netzwerken muss eine Zentrale des Netzwerkes mit dem Router verbunden sein, damit Daten übertragen werden können. Über diese Verbindung werden sämtliche erfassten Daten aus dem Netzwerk übertragen.

### Remote Maintenance für Remote Portal

Remote Maintenance erfasst Daten von relevanten LSN-Geräten und Funktionsmodulen und sendet diese an das Remote Portal, wo sie analysiert und für Wartungsaktivitäten visuell dargestellt werden.

### Remote Maintenance für privates Sicherheitsnetzwerk

Remote Maintenance kann für Private Secure Network konfiguriert werden: Erfasste Daten werden an ein zentrales Managementserversystem (CMS) gesendet.



### Vorsicht!

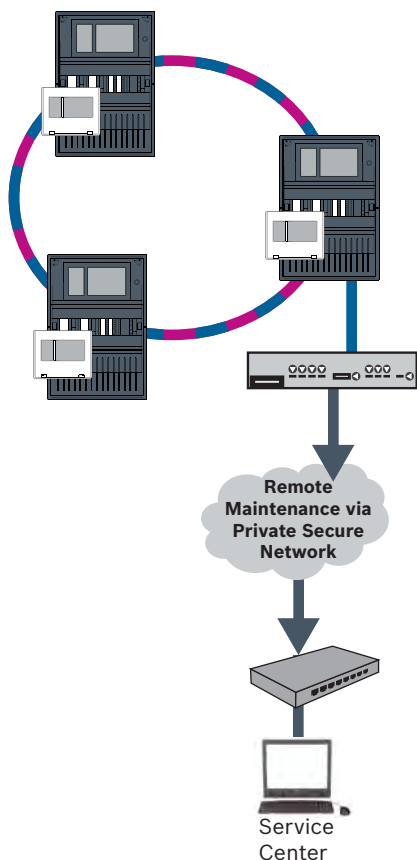
Remote Services erfordert eine sichere IP-Verbindung. Bosch Remote Services oder Verbindung mit Private Secure Network ist erforderlich.

Mit Private Secure Network wird ein IP-Netzwerk auf DSL-Basis mit einem optionalen drahtlosen Zugriff seitens der Zentrale bereitgestellt (EffiLink). Remote Services für Private Secure Network ist in Deutschland nur in Verbindung mit einem Wartungsvertrag für Bosch BT-IE erhältlich.



### Hinweis!

Um Zentralen über FX zu verbinden, verwenden Sie von Bosch zugelassene Medienkonverter.



**Abbildung 8.5: Remote Maintenance für privates Sicherheitsnetzwerk**

Für Remote Maintenance müssen Sie die Server-IP-Adresse und den Port des Remote Maintenance-Systemservers in der Programmiersoftware FSP-5000-RPS eintragen. Vergeben Sie für das Netzwerk eine eindeutige Zentralennetzwerk-ID.

#### **Der Switch zur Anbindung des CMS muss separat programmiert werden.**

Programmieren Sie die IP-Adresse und Redundanzeinstellungen des Switch (siehe *Einstellungen am Switch, Seite 45*). Da der Switch in unmittelbarer Nähe (ohne Zwischenraum) installiert ist, muss die Stromversorgung nicht redundant ausgeführt werden, und die Störungsausgänge werden dementsprechend nicht genutzt.

Achten Sie darauf, dass die RSTP-Einstellungen in den Zentralensteuerungen, in FSP-5000-RPS und im Ethernet-Switch gleich sind.

## 8.4 Remote Portal

### Anforderungen



#### Hinweis!

Um Neukonfigurationen oder Anpassungen bei der Verwendung von Remote Services zu vermeiden, stellen Sie sicher, dass die folgenden Anforderungen erfüllt sind:

- Zentrale mit Firmware 2.19.7 oder höher, alle Zentralen über Ethernet verbunden, Ethernet-Schnittstellen aktiviert und Standard-Ethernet-Einstellungen
- Remote Connect in der FSP-5000-RPS Zentralenkonfiguration aktiviert
- Sicheres Netzwerk-Gateway für Remote Services verfügbar
- Computer mit FSP-5000-RPS 4.8 oder höher und Internetzugang



#### Hinweis!

Vermeiden Sie die Aktualisierung des sicheren Netzwerk-Gateways während der Verbindung. Aktualisierungen des sicheren Netzwerk-Gateways werden regelmäßig in den frühen Morgenstunden ausgeführt. Geben Sie dazu die Zeitzone unter **System** -> **General Settings** (Allgemeine Einstellungen) -> **Timezone** (Zeitzone) an.

### Anweisungen

Um Remote Services zu verwenden, müssen Sie ein Remote Portal-Benutzerkonto haben.

#### Schritt 1: Erstellen Sie ein Remote Portal-Konto

Sie können mehrere Benutzer unter einem Remote Portal-Konto haben. Jedes Remote Portal-Konto hat eine eindeutige Remote ID, die dafür da ist, ein ganzes Unternehmen zu repräsentieren. Wenn Sie kein bestehendes Remote Portal-Konto verwenden können, müssen Sie eins erstellen:

1. Unter <https://remote.boschsecurity.com> -> **Sign up** (Anmelden) geben Sie Ihren Namen, Ihr Unternehmen und Ihre E-Mail-Adresse an, um ein Passwort zu erstellen. Beachten Sie die allgemeinen Geschäftsbedingungen und wählen Sie **I agree to the terms and conditions** (Allgemeinen Geschäftsbedingungen zustimmen). Beachten Sie auch die Datenschutzerklärung und wählen Sie **I agree to the privacy statement** (Datenschutzerklärung zustimmen).
2. Klicken Sie auf **Register** (Registrieren).  
Das Remote Portal sendet umgehend eine E-Mail mit dem Aktivierungslink an die angegebene Adresse.
3. Zur Aktivierung des Kontos klicken Sie auf den Aktivierungslink. Klicken Sie auf dem Remote Portal auf Ihren Benutzernamen und wählen Sie **Account Settings** (Kontoeinstellungen). Hier finden Sie Ihre Remote ID. Sie benötigen diese Remote ID zu einem späteren Zeitpunkt in der Zentralensteuerung.

Um jedem Techniker ein eigenes Konto zu geben, erstellen Sie mehrere Benutzer für dieselbe Remote ID:

Sie werden beim Remote Portal angemeldet.

- ▶ Wählen Sie **Users** (Benutzer) -> **New Technician** (Neuer Techniker). Geben Sie dann die erforderlichen Daten ein, und bestätigen Sie mit **Save** (Speichern).

#### Schritt 2: Sicheres Netzwerk-Gateway verbinden

Um Remote Services einzurichten, verwenden Sie ein sicheres Netzwerk-Gateway.

1. Verbinden Sie den WAN-Port des sicheren Netzwerk-Gateways mit dem Internetrouter oder dem Unternehmensnetzwerk, das den Internetzugang bereitstellt.

- Überprüfen Sie auf dem Internetrouter oder im Unternehmensnetzwerk die Verfügbarkeit der folgenden Protokolle und Ports für das sichere Netzwerk-Gateway (zur Anschaltung an Remote Services erforderlich).

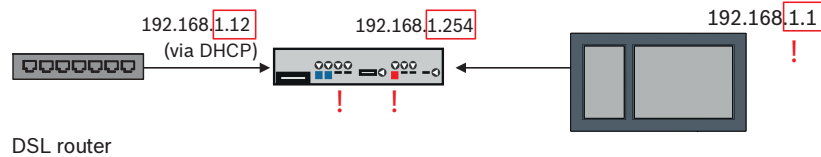
Protokoll	Standard-Port	Beschreibung
HTTP	80 and 8080	für Remote Connect-Registrierung und Remote Maintenance
IPsec VPN	UDP 500 und UDP 4500	für Remote Connect

- Verbinden Sie den LAN1-Port des sicheren Netzwerk-Gateways mit dem designierten Ethernetport der Zentralensteuerung mithilfe des mitgelieferten CAT5 RJ45-Netzwerkkabels. Schauen Sie sich die möglichen Topologien an.
- Verbinden Sie das sichere Netzwerk-Gateway mit einem 100 V - 230 V Netzanschluss mithilfe des im Lieferumfang enthaltenen Netzteils.  
WAN-LED eingeschaltet (blau), wenn die Verbindung mit dem Internet hergestellt wurde. VPN-LED eingeschaltet (blau) kurz danach zeigt an, dass eine VPN-Verbindung mit dem Remote Portal hergestellt wurde.

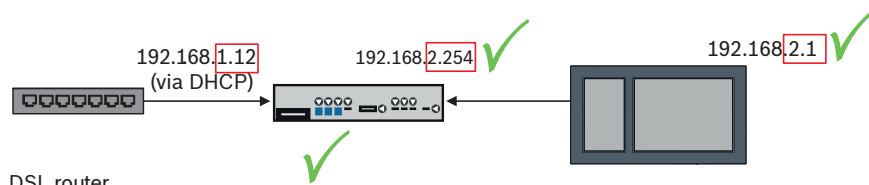
Jede angeschlossene Zentrale oder jedes Zentralennetzwerk hat eine eindeutige System ID.

**Sub-Netzwerke trennen (VPN-LED ausgeschaltet)**

Die Verbindung mit einem sicheren Netzwerk-Gateway für Remote Services schlägt fehl, wenn überlappende Sub-Netzwerke vorhanden sind (VPN-LED ausgeschaltet). Im folgenden Beispiel werden ein sicheres Netzwerk-Gateway und eine Zentralensteuerung gezeigt, die denselben Adressbereich wie der DSL-Router aufweisen.



DSL router



DSL router

Ein sicheres Netzwerk-Gateway mit der neuesten Firmware erkennt überlappende Sub-Netzwerke eindeutig: Die Alarm-LED blinkt kontinuierlich. Sub-Netzwerke werden durch Ändern des dritten Oktetts der IP-Adresse getrennt. Sie ändern die IP-Adressen seitens des Zentralennetzwerks. Nach Ändern der IP-Adresse müssen Sie die Änderungen an das sichere Netzwerk-Gateway weitergeben. Um dies zu tun, müssen Sie die Web-Anwendung über einen Internetbrowser starten.  
- Adresse: <https://192.168.1.254>

- Benutzername: bosch
- Passwort: ipti83

Unter **Configuration** (Konfiguration) -> **Network (LAN)** (Netzwerk (LAN)) können Sie die IP-Adresse ändern. Denken Sie daran, dass die **Standard-Gateway**-Adresse in der Zentralensteuerungskonfiguration die gleiche IP-Adresse haben muss wie das sichere Netzwerk-Gateway.

### Schritt 3: Eine Fernverbindung aufbauen

1. Verwenden Sie die Standard-Ethernet-Einstellungen für die Zentrale.
2. Starten Sie die Zentrale neu.
3. Wählen Sie für die Authentifizierung **Configuration** (Konfiguration) -> **Network Services** (Netzwerkdienste) -> **Change date / time** (Datum/Zeit ändern), und geben Sie das aktuelle Datum ein, und bestätigen Sie die Einstellungen.
4. Wählen Sie **Configuration** (Konfiguration) -> **Network Services** (Netzwerkdienste) -> **Remote Services** und geben dann die Remote ID ein.

Sie können den Status der Remote-Verbindung überprüfen: Wählen Sie in der Zentralensteuerung **Diagnostics** -> **Network Services** -> **Remote Services**.

### Schritt 4: Ordnen Sie die Lizenz im Remote Portal zu.

Um die Verwendung der Remote Services zu aktivieren, müssen Sie im Remote Portal eine Lizenz zuordnen. Eine Lizenz wird für Ihr Konto automatisch mit der ersten erfolgreichen Verbindung bereitgestellt.



#### Hinweis!

Eine bereits zugewiesene Lizenz kann nicht noch einmal zugewiesen werden oder ausgesetzt werden.

1. Geben Sie unter <https://remote.boschsecurity.com> -> **Login** (Anmelden) Ihre E-Mail-Adresse und Ihr Passwort ein.
2. Wählen Sie **Systems** (Systeme).
3. Wählen Sie das System.
4. Klicken Sie unter **Services** (Dienste) auf die Schaltfläche **Add Service** (Dienst hinzufügen) unterhalb des Dienstes.
5. Die Lizenz wird standardmäßig automatisch erneuert (**Service Settings** (Dienst-Einstellungen), Option **With Auto-Renew** (mit autom. Verlängerung)).
6. Bestätigen Sie Ihre Einstellungen mit **Save** (Speichern).

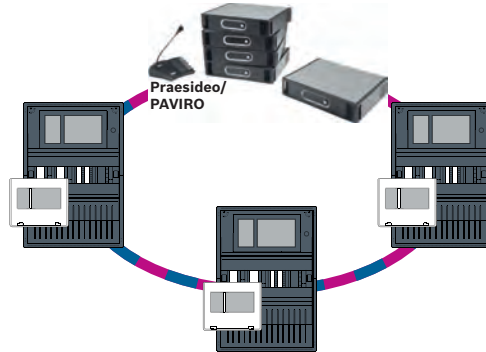
Nach dem Zuordnen der Lizenz können Sie den entsprechenden Dienst verwenden. Eine zugeordnete Lizenz wird durch ein grünes Häkchen angezeigt.

### Schritt 5: Lizenz neu bestellen

1. Bestellen Sie Ein-Jahres-Lizenzen bei Bosch Brandmeldesysteme. Jedes Netzwerk erfordert eigene Lizenzen.  
Bosch sendet eine E-Mail an die angegebene Adresse. Die E-Mail umfasst eindeutige Lizenznummern für die Anzahl von Lizenzen, die Sie bestellt haben, sowie eine Anleitung und einen Link zum Remote Portal.
2. Geben Sie unter <https://remote.boschsecurity.com> -> **Login** (Anmelden) Ihre E-Mail-Adresse und Ihr Passwort ein.
3. Wählen Sie **Licenses** (Lizenzen).
4. Klicken Sie auf die Schaltfläche **+**.
5. Befolgen Sie die Anweisungen im Fenster **Add Licenses** (Lizenzen hinzufügen), und bestätigen Sie mit **Save** (Speichern).
6. Die Liste der Lizenzen wurde aktualisiert.

## 9 Sprachalarmierungssysteme

Die folgende Topologie zeigt über Ethernet angeschaltete Zentralensteuerungen, bei denen das Praesideo/PAVIRO-System über eine Ethernet-Schnittstelle in den Zentralenring integriert wurde.

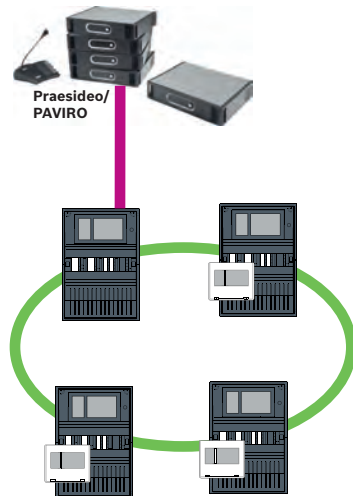


**Abbildung 9.1: Ethernet-Ring mit Praesideo/PAVIRO**

Verwenden Sie den Ethernet Switch (im Allgemeinen MM BPA-ESWEX-RSR20), freigegeben mit Zentralen-Firmwareversion 2.8.

Um zu verhindern, dass EN 54-2-relevanter Multicast-Verkehr zum Praesideo/PAVIRO-System gesendet wird, aktivieren Sie IGMP Snooping des MM. Weitere Informationen finden Sie im entsprechenden Abschnitt des Kapitels zur Installation im Handbuch Vernetzung.

In jeder Zentralensteuerung eines CAN-Netzwerks können Sie ein Praesideo/PAVIRO-System mit einer Ethernet-Schnittstelle verbinden. Die folgende Topologie zeigt über CAN angeschaltete Zentralensteuerungen, bei denen das Praesideo/PAVIRO-System über eine Ethernet-Schnittstelle an eine Zentralensteuerung angeschaltet wurde.



**Abbildung 9.2: Praesideo/PAVIRO-Anschaltung an ein CAN-Netzwerk**



**Hinweis!**

Damit CAN-Netzwerkverkehr nicht über die Ethernet-Verbindung übertragen wird, müssen Sie das Netzwerk über IP in der FSP-5000-RPS Programmierungssoftware ausschalten. Wenn dies nicht ausgeschaltet wird, ist das Netzwerk nicht EN 54-konform.



**Hinweis!**

Wenn eine MPC-xxxx-B-Zentralensteuerung für die direkte Anschaltung an ein Praesideo/PAVIRO-System verwendet werden soll, ist ein Crossover-Patchkabel erforderlich, da weder Praesideo/PAVIRO noch die MPC-xxxx-B Auto-MDI(X) unterstützt.

## 10 Installation

### Checkliste

Bevor Sie mit der Installation des Netzwerks beginnen, überprüfen Sie bitte die unten aufgeführten Punkte.

- Ethernet und CAN
  - Die erforderlichen Leitungslängen der Ethernet-TX-, Ethernet-FX- sowie CAN-TX- und CAN-FX-Kabel sind kleiner als deren maximale Länge.
  - Die gesamte Peripherie und Verkabelung der einzelnen Zentralen sind projektiert.
- Netzwerkplanung
  - Alle IP-Adressen und Netzwerkeinstellungen für die einzelnen Zentralen und die zusätzlichen Netzwerkkomponenten sind geplant und stehen zur Verfügung.
  - Eine Übersicht über die zu installierenden Zusatzkomponenten, wie Ethernet-Switches und Medienkonverter, und deren Verkabelung zu benachbarten Zentralen steht Ihnen zur Verfügung.
  - Eine Übersicht über die zu installierende Netzwerktopologie steht Ihnen zur Verfügung.
  - Alle Netzwerkredundanzeinstellungen müssen geplant und verfügbar sein.

### 10.1 Einstellungen auf Medienkonvertern

Für die Verwendung des Medienkonverters sind nur wenige Schritte erforderlich:

- Stellen Sie die DIP-Schalter ein.
- Verbinden Sie den Medienkonverter mit den FX-Netzwerkkabeln und den CAT5e-Netzwerkkabeln.
- Versorgen Sie den Medienkonverter über das interne BCM Batterieregler-Modul mit Strom.



#### Hinweis!

Die Medienkonverter werden nur über den Energieversorgungsanschluss 1 mit Strom versorgt.

Die Fehler-LED des Medienkonverters leuchtet deshalb kontinuierlich. Dies hat jedoch keinen Einfluss auf die Funktionsfähigkeit des Geräts.



#### Hinweis!

Verwenden Sie für die Vernetzung nur folgende Kabel:

Ethernet-Kabel

Ethernet-Patchkabel, geschirmt, CAT5e oder besser.

Beachten Sie die in der Kabelspezifikation angegebenen minimalen Biegeradien.

Lichtwellenleiter

Multimode: Lichtwellenleiter-Ethernet-Patchkabel, Duplex I-VH2G 50/125µ oder Duplex I-VH2G 62,5/125µ, SC-Stecker

Singlemode: Lichtwellenleiter-Ethernet-Patchkabel, Duplex I-VH2E 9/125µ

Beachten Sie die in der Kabelspezifikation angegebenen minimalen Biegeradien.



#### Hinweis!

Informationen zum Einbau der Medienkonverter in die Gehäuse der Zentrale finden Sie in den Installationsanleitungen zu den Montagesätzen:FPM 5000

KMC(F.01U.266.845)FPM-5000-KES(F.01U.266.844)



**Hinweis!**

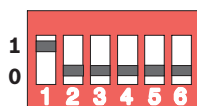
Der maximale Übertragungsabschnitt der Multimode-Medienkonverter über FX beträgt 2000 m.

Der maximale Übertragungsabschnitt der Singlemode-Medienkonverter über FX beträgt 40 km.

Konfigurieren Sie den Medienkonverter mithilfe der DIP-Schalter wie folgt:

**Hinweis!**

Verändern Sie die DIP-Schalter-Einstellungen nur an spannungsfreien Medienkonvertern.



DIP-Schalturnummer	Einstellung
1	Link-Fault-Pass-Through eingeschaltet
2	Ethernet: Automatischer Modus
3	Ethernet: 100 MBit
4	Ethernet: Voll-Duplex
5	Lichtwellenleiter: Voll-Duplex
6	Link Down: Aus

**10.2****Installieren des Ethernet-Switch****Warnung!**

Laserlicht

Nicht in den Strahl blicken oder direkt mit optischen Instrumenten (z. B. Lupe, Mikroskop) betrachten. Das Nichtbeachten dieses Hinweises kann Ihre Augen gefährden, wenn der Abstand weniger als 100 mm beträgt. Das Licht tritt an den optischen Anschlüssen oder am Ende der daran angeschlossenen Lichtwellenleiter aus. Diode Klasse 2M, Wellenlänge 650 nm, Leistung < 2 mW, gemäß IEC 60825-1.

**Hinweis!**

Informationen finden Sie in der Installationsanleitung für den Montagesatz für Ethernet-Switch FPM-5000-KES (F.01U.260.523).

**10.3****Einstellungen am Switch**

Um die Switches im Netzwerk verwenden zu können, müssen Sie diese programmieren. Verbinden Sie einen Laptop mit dem Netzwerk und verwenden Sie für die Erstprogrammierung die vom Hersteller mitgelieferte Software HiDiscovery. Suchen Sie mithilfe dieser Software nach den Switches im Netzwerk. Doppelklicken Sie auf den Switch, um ihn auszuwählen, und weisen Sie ihm eine IP-Adresse zu.

Nach der Erstprogrammierung der IP-Adresse können Sie einen Web-Browser verwenden, um die Konfigurationsoberfläche des Switches aufzurufen.

**Hinweis!**

Eine genaue Beschreibung der Installation und Konfiguration der Switches finden Sie in der Bedienungsanleitung des Herstellers. Zugangsdaten:

Benutzer: admin

Passwort: private

Verwenden Sie einen Browser, um die Konfigurationsoberfläche für die Switches aufzurufen. Zu diesem Zweck müssen Sie folgende Einstellungen im Switch vornehmen:

- *IP-Adresse vergeben, Seite 46*
  - *Redundanzeinstellungen programmieren, Seite 47*
- Weitere optionale Einstellungen, z. B.:
- *Fehlerrelais programmieren, Seite 47*
  - *Verbindungsüberwachung programmieren, Seite 48*
  - *IGMP Snooping aktivieren, Seite 48*

**10.3.1****IP-Adresse vergeben****Hinweis!**

Praxistipp:

Wenn es die Netzwerkkonfiguration erlaubt, verwenden Sie im Geräteteil der IP-Adressen für die Switches Nummern über 200 (xxx.xxx.xxx.200). So erhalten Sie eine klarere Trennung von der Host-ID einer IP-Adresse.

**Beispiel:**

Der Zentrale mit der IP-Adresse 192.168.1.1 ist der Switch 192.168.1.201 zugeordnet.

**Hinweis!**

Eine genaue Beschreibung der Installation und Konfiguration der Switches finden Sie in den folgenden Herstellerdokumenten:

Anwender-Handbuch Installation

Referenz-Handbuch Web-based Interface

Verwenden Sie einen Browser, um die Benutzeroberfläche für die Konfiguration des Switch aufzurufen.

Stellen Sie im Menü **Basic Settings -> Network** (Grundeinstellungen -> Netz) die folgenden Werte entsprechend der gewählten Topologie ein:

- Modus: Lokal
- IP-Adresse: die gewünschte IP-Adresse, z. B. 192.168.1.201
- Netzmaske: die gewünschte Netzmaske, z. B. 255.255.255.0
- Gateway: das gewünschte Gateway, z. B. 192.168.1.254 oder 0.0.0.0, wenn kein Gateway benötigt wird.

Klicken Sie auf **Schreiben** (Write).

**Hinweis!**

Die Einstellungen in den einzelnen Menüpunkten der Switch-Konfiguration werden nach dem Klicken auf **Schreiben** (Write) wirksam.

Die Einstellungen werden nur dauerhaft gespeichert, das heißt, sie bleiben nach dem Neustart des Gerätes nur dann erhalten, wenn Sie unter **Grundeinstellungen (Basic Settings) -> Laden/Speichern** (Load/Save) im Feld **Speichern** (Save) die Option **Auf dem Gerät** (On the device) auswählen und auf die Schaltfläche **Sichern** (Save) klicken.

### 10.3.2 Redundanzeinstellungen programmieren

Da die FPA-Zentralennetzwerke RSTP als Redundanzprotokoll verwenden, müssen Sie das Protokoll in der Konfigurationsoberfläche aktivieren und programmieren:

Stellen Sie im Menü **Redundanz -> Spanning Tree -> Global** die folgenden Werte ein:

- Funktion: An
- Protokollversion: RSTP
- Protokollkonfiguration: Verwenden Sie die gleichen Einstellungen wie bei den Zentralensteuerungen.

Klicken Sie auf **Schreiben**.



#### Hinweis!

Die Einstellungen in den einzelnen Menüpunkten der Switch-Konfiguration werden nach dem Klicken auf **Schreiben** wirksam.

Die Einstellungen werden nur dauerhaft gespeichert, das heißt, sie bleiben nach dem Neustart des Gerätes nur dann erhalten, wenn Sie unter **Grundeinstellungen -> Laden/Speichern** im Feld **Speichern** die Option **Auf dem Gerät** auswählen und auf die Schaltfläche **Sichern** klicken.

### 10.3.3 Fehlerrelais programmieren



#### Hinweis!

Das Fehlerrelais muss nur bei Anwendungen programmiert werden, bei denen mindestens eine der folgenden Voraussetzungen erfüllt ist:

Es besteht eine Verbindung zwischen zwei Switches. Dieses ist zum Beispiel bei einem Backbone mit Sub-Ringen möglich.

Die Stromversorgung des Switch wird redundant ausgeführt.



#### Hinweis!

Eine genaue Beschreibung der Installation und Konfiguration der Switches finden Sie in den folgenden Herstellerdokumenten:

Anwender-Handbuch Installation

Referenz-Handbuch Web-based Interface

Verwenden Sie einen Browser, um die Benutzeroberfläche für die Konfiguration des Switch aufzurufen.

Setzen Sie unter **Diagnose (Diagnosis) -> Meldekontakt (Signal Contact)** in der Registerkarte **Meldekontakt 1** (Signal Contact 1) den **Modus - Meldekontakt** (Mode Signal Contact) auf **Gerätstatus** (Device Status).

Stellen Sie unter **Diagnose (Diagnosis) -> Gerätstatus (Device Status)** im Feld **Überwachung** (Monitoring) die folgenden Werte ein:

- **Stromversorgung 1** (Power Supply 1): **Überwachen** (Monitor)
- **Verbindungsfehler** (Connection Error): **Überwachen** (Monitor)

Alle anderen Einstellungen müssen auf **Ignorieren** (Ignore) eingestellt sein.



#### Hinweis!

Die Einstellungen unter **Gerätstatus** (Device Status) gelten auch für die Störungs-LED des Switch.

Klicken Sie auf **Schreiben** (Write).

**Hinweis!**

Die Einstellungen in den einzelnen Menüpunkten der Switch-Konfiguration werden nach dem Klicken auf **Schreiben** (Write) wirksam.

Die Einstellungen werden nur dauerhaft gespeichert, das heißt, sie bleiben nach dem Neustart des Gerätes nur dann erhalten, wenn Sie unter **Grundeinstellungen (Basic Settings) -> Laden/Speichern** (Load/Save) im Feld **Speichern** (Save) die Option **Auf dem Gerät** (On the device) auswählen und auf die Schaltfläche **Sichern** (Save) klicken.

**10.3.4****Verbindungsüberwachung programmieren****Hinweis!**

Sie benötigen die Einstellung der Verbindungsüberwachung nur, wenn Sie das Fehlerrelais des Switch verwenden.

Wenn Sie die Verbindungen des Switch mit dem Fehlerrelais überwachen wollen, müssen Sie in der Konfiguration des Switch angeben, welche Ports des Switch überwacht werden sollen. Aktivieren Sie das Kontrollkästchen **Verbindungsfehler weiterleiten** für die einzelnen Ports im Menü **Grundeinstellungen -> Portkonfiguration**.

Nur Anschlüsse, bei denen **Verbindungsfehler weiterleiten** aktiviert wurde, werden überwacht.

Klicken Sie auf **Schreiben**.

**Hinweis!**

Die Einstellungen in den einzelnen Menüpunkten der Switch-Konfiguration werden nach dem Klicken auf **Schreiben** wirksam.

Die Einstellungen werden nur dauerhaft gespeichert, das heißt, sie bleiben nach dem Neustart des Gerätes nur dann erhalten, wenn Sie unter **Grundeinstellungen -> Laden/Speichern** im Feld **Speichern** die Option **Auf dem Gerät** auswählen und auf die Schaltfläche **Sichern** klicken.

**10.3.5****QoS-Priorität, nur bei UGM-2040**

Wenn Sie die Switches für die Kommunikation zwischen FPA-Netzwerken und der UGM-2040 verwenden, muss die QoS-Priorität in den Switches der UGM eingestellt werden.

Ändern Sie im Menü QoS/Priorität -> Global die Einstellungen des Dropdown-Listenfeldes unter Trusted Mode auf trustIpDscp.

Klicken Sie auf **Schreiben**.

**Hinweis!**

Die Einstellungen in den einzelnen Menüpunkten der Switch-Konfiguration werden nach dem Klicken auf **Schreiben** wirksam.

Die Einstellungen werden nur dauerhaft gespeichert, das heißt, sie bleiben nach dem Neustart des Gerätes nur dann erhalten, wenn Sie unter **Grundeinstellungen -> Laden/Speichern** im Feld **Speichern** die Option **Auf dem Gerät** auswählen und auf die Schaltfläche **Sichern** klicken.

**10.3.6****IGMP Snooping aktivieren**

Um zu verhindern, dass EN 54-2 relevanter Multicast-Verkehr zu anderen Systemen geht, die mit dem Ethernet Switch (Praesideo/PAVIRO, Remote Connect) verbunden sind, aktivieren Sie IGMP Snooping.

Wählen Sie auf der IGMP-Konfigurationsseite des Ethernet Switch die folgenden Optionen:

1. Schalten Sie den **IGMP Snooping**-Betrieb ein.

2. Steuern Sie den **IGMP Querieran**.
3. Konfigurieren Sie das Übertragungsintervall, in dem der RSR20 IGMP-Abfragepakete sendet (z. B. 4 Sekunden).
4. Konfigurieren Sie die Zeit, innerhalb der Multicast-Gruppenmitglieder auf IGMP-Abfragen reagieren sollen (z. B. 3 Sekunden).
5. Wählen Sie **Verwerfen** für Pakete mit unbekanntem Multicast-Adressen.
6. Wählen Sie **An Query und registrierte Ports senden** für Pakete mit bekannten Multicast-Adressen.
7. Aktivieren Sie IGMP nur für Ports, an denen andere Systeme mit dem Switch verbunden sind. Deaktivieren Sie die Option **Statischer Query Port** für alle Ports.

## 10.4

### CAN-Netzwerk

#### Vernetzung und Schnittstellen

Die Zentralensteuerung verfügt über

- zwei CAN-Schnittstellen (CAN1/CAN2) zur Vernetzung (Ring- oder Stich-Topologie)
- zwei Signaleingänge (IN1/IN2)
- zwei Ethernet-Schnittstellen
- USB-Schnittstelle

Abhängig vom Zentralensteuerungstyp:

- zwei weitere Ethernet-Schnittstellen
- RS232-Schnittstelle

Beachten Sie die maximale Leitungslänge von 3 m bei Anschluss an die USB- und von 2 m bei Anschluss an die RS232-Schnittstelle.

#### Adressvergabe und Einstellungen im Netzwerk

Abhängig vom Zentralensteuerungstyp:

- Physikalische Knotenadresse, die beim ersten Einschalten der Zentrale in der Zentralen-Firmware festgelegt wird.
- RSN an den mechanischen Drehschaltern auf der Rückseite der Zentrale

Anzeige der physikalischen Knotenadresse, wenn sie in der Zentralensteuerung gespeichert ist:

- ▶ Wählen Sie **Konfiguration -> Netzwerkdienste -> Ethernet -> Ethernet-Einstellungen verwenden -> IP-Einstellungen -> Standardeinst.**

So ändern Sie die physikalische Knotenadresse, die in der Zentralensteuerung gespeichert ist:

- ▶ Zeigen Sie die Standardeinstellungen an und ändern Sie die letzte Zahl der **IP-Adresse**.

So ändern Sie die mechanische RSN:

- ▶ Sie können die RSN auf mechanischen Drehschaltern auf der Rückseite der Zentrale festlegen. Notieren Sie sie auf dem Schild unter den Drehschaltern.

#### Konfiguration der Topologie

Die DIP-Schalter für die Konfiguration verschiedener Topologien befinden sich auf der Rückseite.

- ▶ Markieren Sie die gewählte Einstellung auf dem Schild neben den DIP-Schaltern.

### Stand-Alone-Zentrale und Stand-Alone-Zentrale redundant

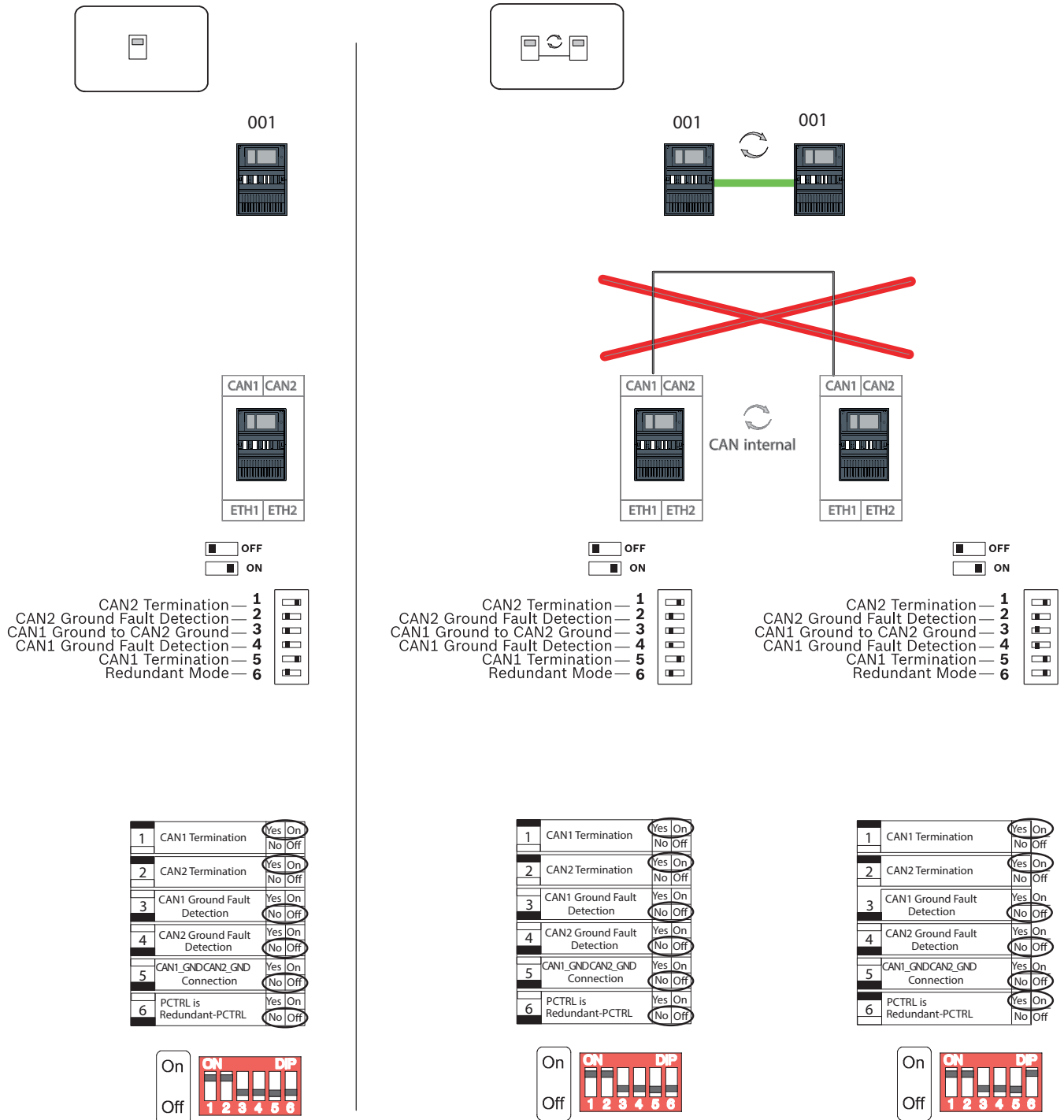
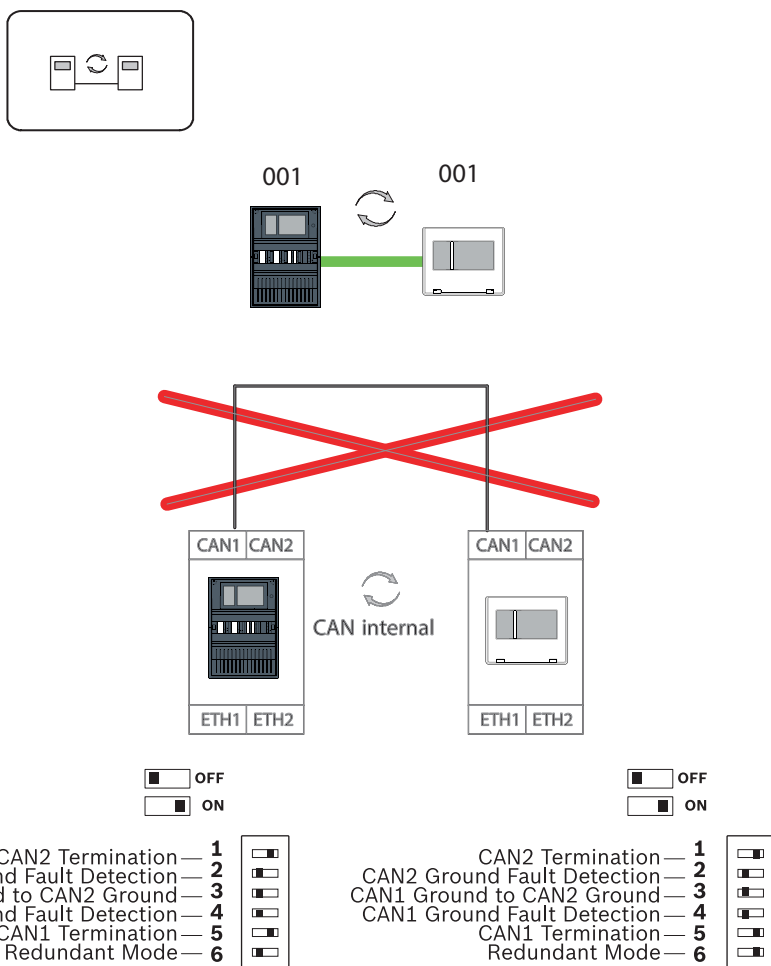


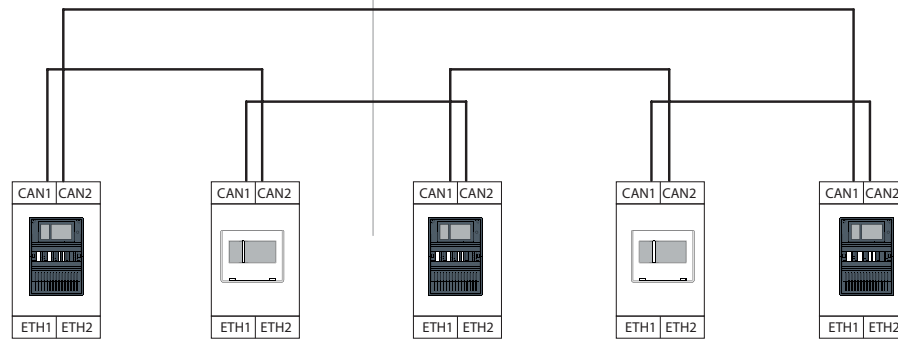
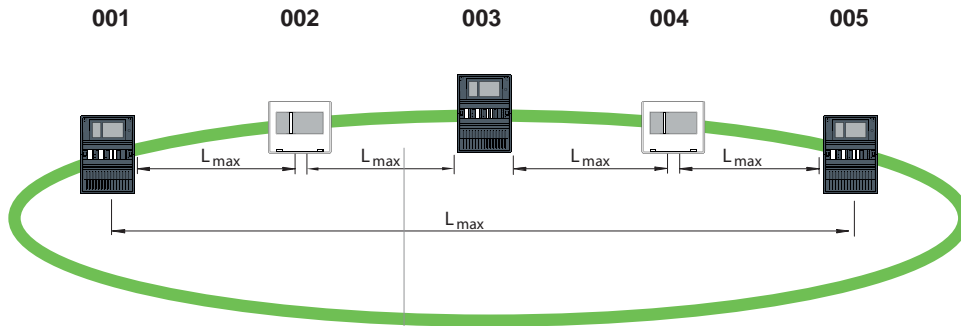
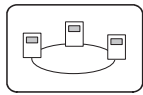
Abbildung 10.1: DIP-Schaltereinstellungen für Stand-Alone-Zentrale (oben: AVENAR, unten: FPA, links: regulär, rechts: redundant)

### Abgesetzte Bedieneinheit als redundante Zentrale



**Abbildung 10.2: DIP-Schaltereinstellungen für abgesetzte Bedieneinheit als redundante Zentrale (nur AVENAR)**

**Ring**



Legend for DIP switches:

- OFF (white square)
- ON (black square)

CAN2 Termination	1	<input type="checkbox"/>
CAN2 Ground Fault Detection	2	<input type="checkbox"/>
CAN1 Ground to CAN2 Ground	3	<input type="checkbox"/>
CAN1 Ground Fault Detection	4	<input type="checkbox"/>
CAN1 Termination	5	<input type="checkbox"/>
Redundant Mode	6	<input type="checkbox"/>

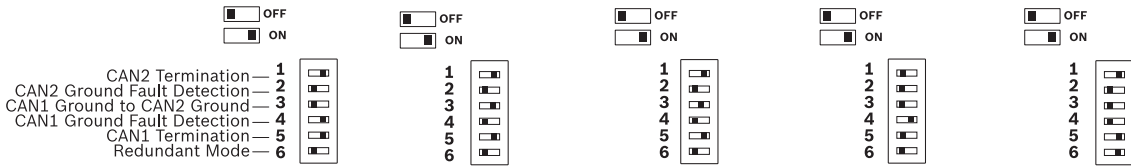
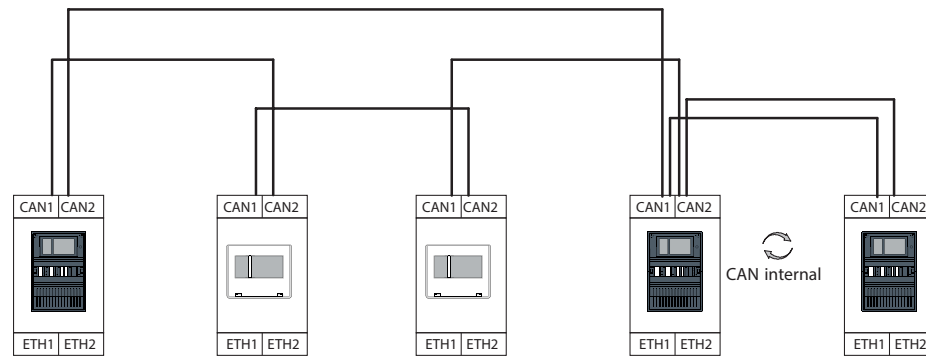
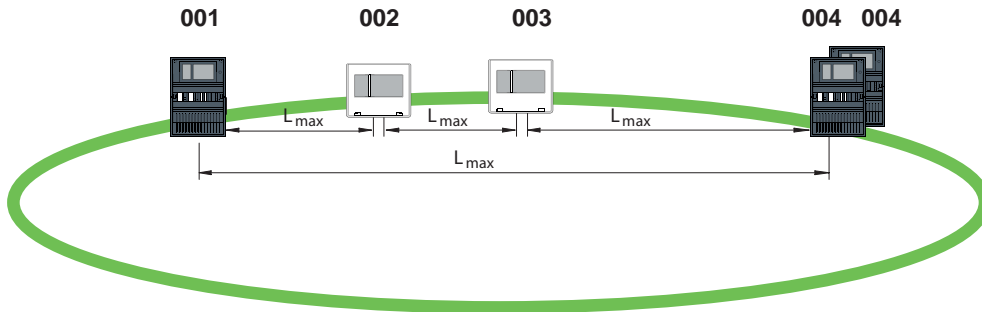
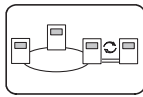
<table border="1"> <tr><td>1</td><td>CAN1 Termination</td><td>Yes/On</td><td>No/Off</td></tr> <tr><td>2</td><td>CAN2 Termination</td><td>Yes/On</td><td>No/Off</td></tr> <tr><td>3</td><td>CAN1 Ground Fault Detection</td><td>Yes/On</td><td>No/Off</td></tr> <tr><td>4</td><td>CAN2 Ground Fault Detection</td><td>Yes/On</td><td>No/Off</td></tr> <tr><td>5</td><td>CAN1_GND/CAN2_GND Connection</td><td>Yes/On</td><td>No/Off</td></tr> <tr><td>6</td><td>PCTRL is Redundant-PCTRL</td><td>Yes/On</td><td>No/Off</td></tr> </table>	1	CAN1 Termination	Yes/On	No/Off	2	CAN2 Termination	Yes/On	No/Off	3	CAN1 Ground Fault Detection	Yes/On	No/Off	4	CAN2 Ground Fault Detection	Yes/On	No/Off	5	CAN1_GND/CAN2_GND Connection	Yes/On	No/Off	6	PCTRL is Redundant-PCTRL	Yes/On	No/Off	<table border="1"> <tr><td>1</td><td>CAN1 Termination</td><td>Yes/On</td><td>No/Off</td></tr> <tr><td>2</td><td>CAN2 Termination</td><td>Yes/On</td><td>No/Off</td></tr> <tr><td>3</td><td>NA</td><td>Yes/On</td><td>No/Off</td></tr> <tr><td>4</td><td>NA</td><td>Yes/On</td><td>No/Off</td></tr> <tr><td>5</td><td>CAN1_GND/CAN2_GND Connection</td><td>Yes/On</td><td>No/Off</td></tr> <tr><td>6</td><td>NA</td><td>Yes/On</td><td>No/Off</td></tr> </table>	1	CAN1 Termination	Yes/On	No/Off	2	CAN2 Termination	Yes/On	No/Off	3	NA	Yes/On	No/Off	4	NA	Yes/On	No/Off	5	CAN1_GND/CAN2_GND Connection	Yes/On	No/Off	6	NA	Yes/On	No/Off	<table border="1"> <tr><td>1</td><td>CAN1 Termination</td><td>Yes/On</td><td>No/Off</td></tr> <tr><td>2</td><td>CAN2 Termination</td><td>Yes/On</td><td>No/Off</td></tr> <tr><td>3</td><td>CAN1 Ground Fault Detection</td><td>Yes/On</td><td>No/Off</td></tr> <tr><td>4</td><td>CAN2 Ground Fault Detection</td><td>Yes/On</td><td>No/Off</td></tr> <tr><td>5</td><td>CAN1_GND/CAN2_GND Connection</td><td>Yes/On</td><td>No/Off</td></tr> <tr><td>6</td><td>PCTRL is Redundant-PCTRL</td><td>Yes/On</td><td>No/Off</td></tr> </table>	1	CAN1 Termination	Yes/On	No/Off	2	CAN2 Termination	Yes/On	No/Off	3	CAN1 Ground Fault Detection	Yes/On	No/Off	4	CAN2 Ground Fault Detection	Yes/On	No/Off	5	CAN1_GND/CAN2_GND Connection	Yes/On	No/Off	6	PCTRL is Redundant-PCTRL	Yes/On	No/Off	<table border="1"> <tr><td>1</td><td>CAN1 Termination</td><td>Yes/On</td><td>No/Off</td></tr> <tr><td>2</td><td>CAN2 Termination</td><td>Yes/On</td><td>No/Off</td></tr> <tr><td>3</td><td>NA</td><td>Yes/On</td><td>No/Off</td></tr> <tr><td>4</td><td>NA</td><td>Yes/On</td><td>No/Off</td></tr> <tr><td>5</td><td>CAN1_GND/CAN2_GND Connection</td><td>Yes/On</td><td>No/Off</td></tr> <tr><td>6</td><td>NA</td><td>Yes/On</td><td>No/Off</td></tr> </table>	1	CAN1 Termination	Yes/On	No/Off	2	CAN2 Termination	Yes/On	No/Off	3	NA	Yes/On	No/Off	4	NA	Yes/On	No/Off	5	CAN1_GND/CAN2_GND Connection	Yes/On	No/Off	6	NA	Yes/On	No/Off	<table border="1"> <tr><td>1</td><td>CAN1 Termination</td><td>Yes/On</td><td>No/Off</td></tr> <tr><td>2</td><td>CAN2 Termination</td><td>Yes/On</td><td>No/Off</td></tr> <tr><td>3</td><td>CAN1 Ground Fault Detection</td><td>Yes/On</td><td>No/Off</td></tr> <tr><td>4</td><td>CAN2 Ground Fault Detection</td><td>Yes/On</td><td>No/Off</td></tr> <tr><td>5</td><td>CAN1_GND/CAN2_GND Connection</td><td>Yes/On</td><td>No/Off</td></tr> <tr><td>6</td><td>PCTRL is Redundant-PCTRL</td><td>Yes/On</td><td>No/Off</td></tr> </table>	1	CAN1 Termination	Yes/On	No/Off	2	CAN2 Termination	Yes/On	No/Off	3	CAN1 Ground Fault Detection	Yes/On	No/Off	4	CAN2 Ground Fault Detection	Yes/On	No/Off	5	CAN1_GND/CAN2_GND Connection	Yes/On	No/Off	6	PCTRL is Redundant-PCTRL	Yes/On	No/Off
1	CAN1 Termination	Yes/On	No/Off																																																																																																																									
2	CAN2 Termination	Yes/On	No/Off																																																																																																																									
3	CAN1 Ground Fault Detection	Yes/On	No/Off																																																																																																																									
4	CAN2 Ground Fault Detection	Yes/On	No/Off																																																																																																																									
5	CAN1_GND/CAN2_GND Connection	Yes/On	No/Off																																																																																																																									
6	PCTRL is Redundant-PCTRL	Yes/On	No/Off																																																																																																																									
1	CAN1 Termination	Yes/On	No/Off																																																																																																																									
2	CAN2 Termination	Yes/On	No/Off																																																																																																																									
3	NA	Yes/On	No/Off																																																																																																																									
4	NA	Yes/On	No/Off																																																																																																																									
5	CAN1_GND/CAN2_GND Connection	Yes/On	No/Off																																																																																																																									
6	NA	Yes/On	No/Off																																																																																																																									
1	CAN1 Termination	Yes/On	No/Off																																																																																																																									
2	CAN2 Termination	Yes/On	No/Off																																																																																																																									
3	CAN1 Ground Fault Detection	Yes/On	No/Off																																																																																																																									
4	CAN2 Ground Fault Detection	Yes/On	No/Off																																																																																																																									
5	CAN1_GND/CAN2_GND Connection	Yes/On	No/Off																																																																																																																									
6	PCTRL is Redundant-PCTRL	Yes/On	No/Off																																																																																																																									
1	CAN1 Termination	Yes/On	No/Off																																																																																																																									
2	CAN2 Termination	Yes/On	No/Off																																																																																																																									
3	NA	Yes/On	No/Off																																																																																																																									
4	NA	Yes/On	No/Off																																																																																																																									
5	CAN1_GND/CAN2_GND Connection	Yes/On	No/Off																																																																																																																									
6	NA	Yes/On	No/Off																																																																																																																									
1	CAN1 Termination	Yes/On	No/Off																																																																																																																									
2	CAN2 Termination	Yes/On	No/Off																																																																																																																									
3	CAN1 Ground Fault Detection	Yes/On	No/Off																																																																																																																									
4	CAN2 Ground Fault Detection	Yes/On	No/Off																																																																																																																									
5	CAN1_GND/CAN2_GND Connection	Yes/On	No/Off																																																																																																																									
6	PCTRL is Redundant-PCTRL	Yes/On	No/Off																																																																																																																									

Visual representation of the DIP switch settings for each node, showing switches 1-6 in ON or OFF positions.

Abbildung 10.3: DIP-Schaltereinstellungen für Ring (oben: AVENAR, unten: FPA)



### Ring mit redundanten Zentralen



1	CAN1 Termination	Yes/On	No/Off	1	CAN1 Termination	Yes/On	No/Off	1	CAN1 Termination	Yes/On	No/Off	1	CAN1 Termination	Yes/On	No/Off
2	CAN2 Termination	Yes/On	No/Off	2	CAN2 Termination	Yes/On	No/Off	2	CAN2 Termination	Yes/On	No/Off	2	CAN2 Termination	Yes/On	No/Off
3	CAN1 Ground Fault Detection	Yes/On	No/Off	3	NA	Yes/On	No/Off	3	CAN1 Ground Fault Detection	Yes/On	No/Off	3	CAN1 Ground Fault Detection	Yes/On	No/Off
4	CAN2 Ground Fault Detection	Yes/On	No/Off	4	NA	Yes/On	No/Off	4	CAN2 Ground Fault Detection	Yes/On	No/Off	4	CAN2 Ground Fault Detection	Yes/On	No/Off
5	CAN1_GND CAN2_GND Connection	Yes/On	No/Off	5	CAN1_GND CAN2_GND Connection	Yes/On	No/Off	5	CAN1_GND CAN2_GND Connection	Yes/On	No/Off	5	CAN1_GND CAN2_GND Connection	Yes/On	No/Off
6	PCTRL is Redundant-PCTRL	Yes/On	No/Off	6	NA	Yes/On	No/Off	6	PCTRL is Redundant-PCTRL	Yes/On	No/Off	6	PCTRL is Redundant-PCTRL	Yes/On	No/Off

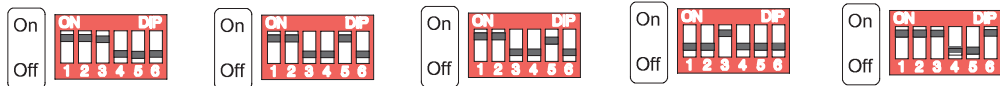
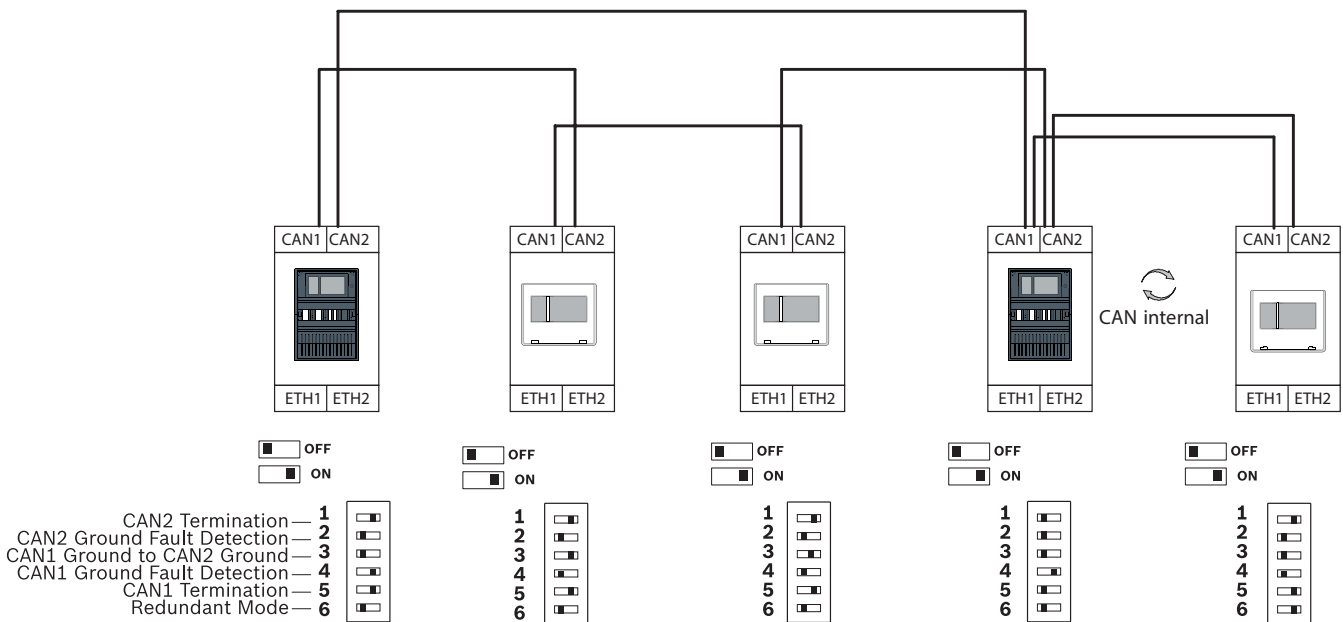
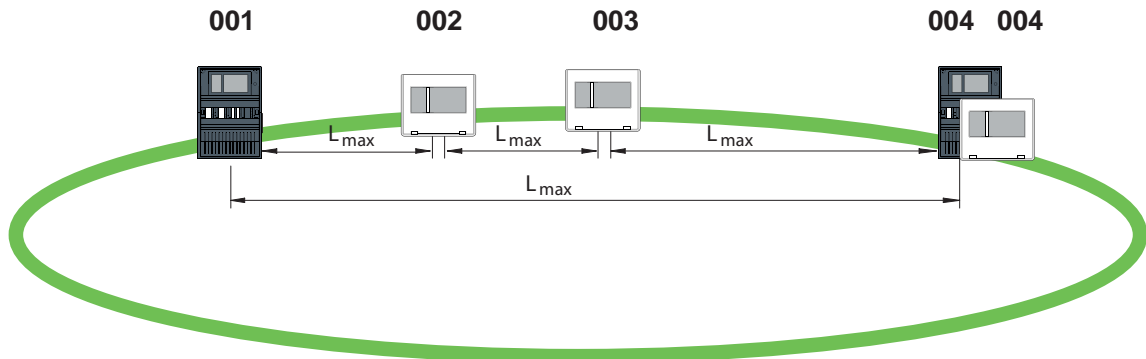
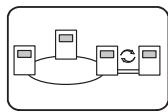


Abbildung 10.4: DIP-Schaltereinstellungen für Ring mit redundanten Zentralen (oben: AVENAR, unten: FPA)

**Ring mit abgesetzter Bedieneinheit als redundante Zentrale**



**Abbildung 10.5: DIP-Schaltereinstellungen für Ring mit abgesetzter Bedieneinheit (nur AVENAR)**

# 11 Verkabelung

Zur Erstellung eines EN 54-2-konformen Systems, schließen Sie die RSTP-Switches und die Medienkonverter über die überwachte Stromversorgung der Brandmelderzentrale an.

- Verwenden Sie für die Stromversorgung der Medienkonverter und der RSTP-Switches den 24V-Ausgang der BCM 0000 B oder FPP-5000.
- Wenn Sie eine redundante Stromversorgung verbunden haben oder eine Verbindung von Switch zu Switch erstellen, müssen die Störungsausgänge des RSTP-Switch über Zentralenausgänge überwacht werden. Verwenden Sie zum Beispiel die Eingänge an der Zentralensteuerung oder IOP 0008 A.
- Beim Medienkonverter muss die Funktion „Link-Fault-Pass-Through“ aktiviert sein. Die Konfiguration erfolgt über den DIP-Schalter des Medienconverters.



**Hinweis!**

Verwenden Sie für die Vernetzung nur folgende Kabel:

Ethernet-Kabel

Ethernet-Patchkabel, geschirmt CAT5e oder besser.

Bitte beachten Sie die in der Kabelspezifikation angegebenen minimalen Biegeradien.

LWL-Kabel

Multi-Mode: Fiber Optic Ethernet-Patchkabel, Duplex I-VH2G 50/125µ oder Duplex I-VH2G 62,5/125µ, SC-Stecker.

Single-Mode: Fiber Optic Ethernet-Patchkabel, Duplex I-VH2E 9/125µ, SC-Stecker.

Bitte beachten Sie die in der Kabelspezifikation angegebenen minimalen Biegeradien.

**11.1**

**Medienkonverter**

**Anschluss von Medienkonvertern**



**Hinweis!**

Beachten Sie beim Anschluss der FX-Verkabelung der Medienkonverter die Übertragungsrichtung der Lichtwellenleiter.

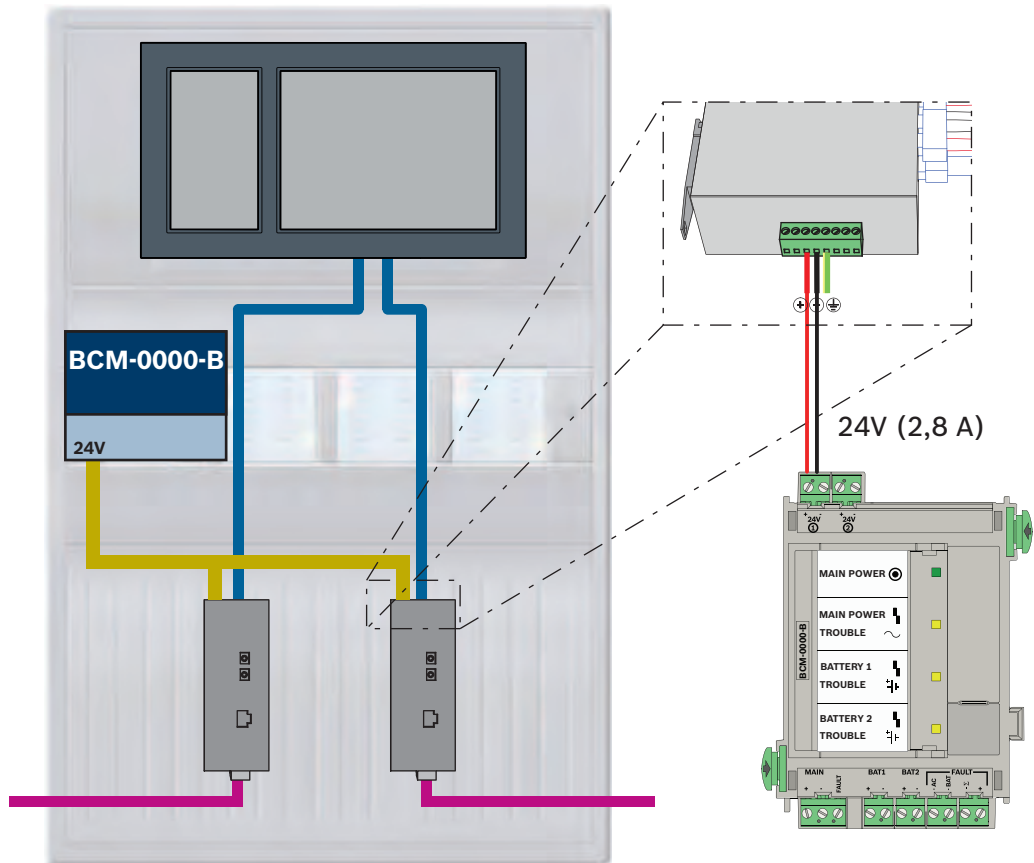





Abbildung 11.1: Anschluss der Medienkonverter an die Stromversorgung und die Zentralensteuerung IN1/ IN2

Symbol	Beschreibung
	Ethernet-Kabel TX (Kupfer)
	Ethernet-Kabel FX (Lichtwellenleiter)

Symbol	Beschreibung
	24-V-Stromversorgung
	Störungsübertragung
	Medienkonverter

## 11.2

### Ethernet-Switch

#### Anschaltung des Switches

Sie können die Störungsausgänge der Switches mit den Eingängen der Zentralensteuerung oder einem IOP-Eingangs-/Ausgangsmodul verbinden.

#### Hinweis!

Das Störungsrelais muss nur bei Anwendungen verbunden werden, bei denen mindestens eine der folgenden Voraussetzungen erfüllt ist:

Es besteht eine Verbindung zwischen 2 Switches. Dieses ist zum Beispiel bei einem Backbone mit Sub-Ringen möglich.

Die Stromversorgung des Switches wird redundant ausgeführt.



**Anschaltung von Switches mit Störungsmeldungen an die Eingänge des IOP-Moduls:**

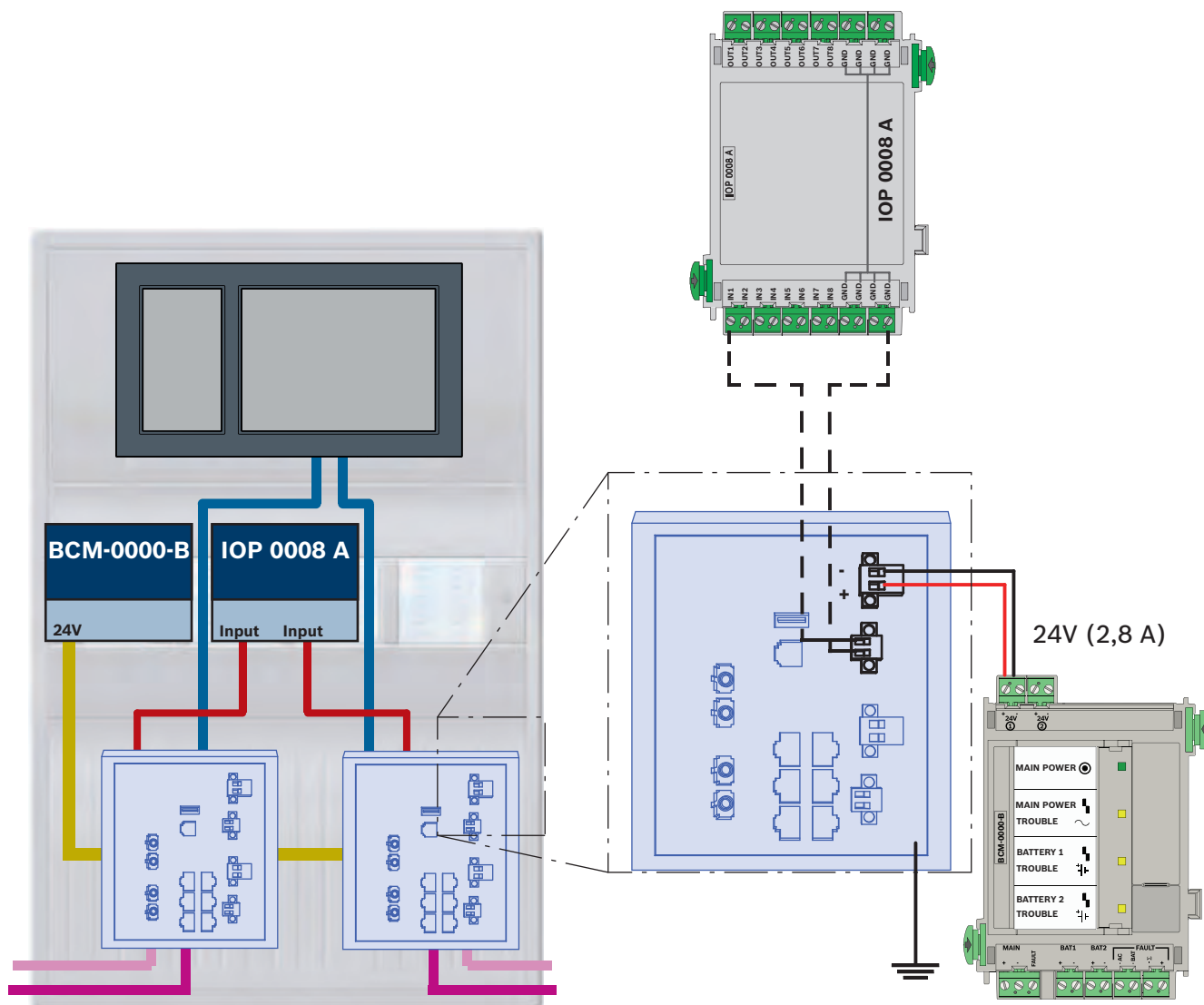




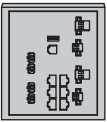
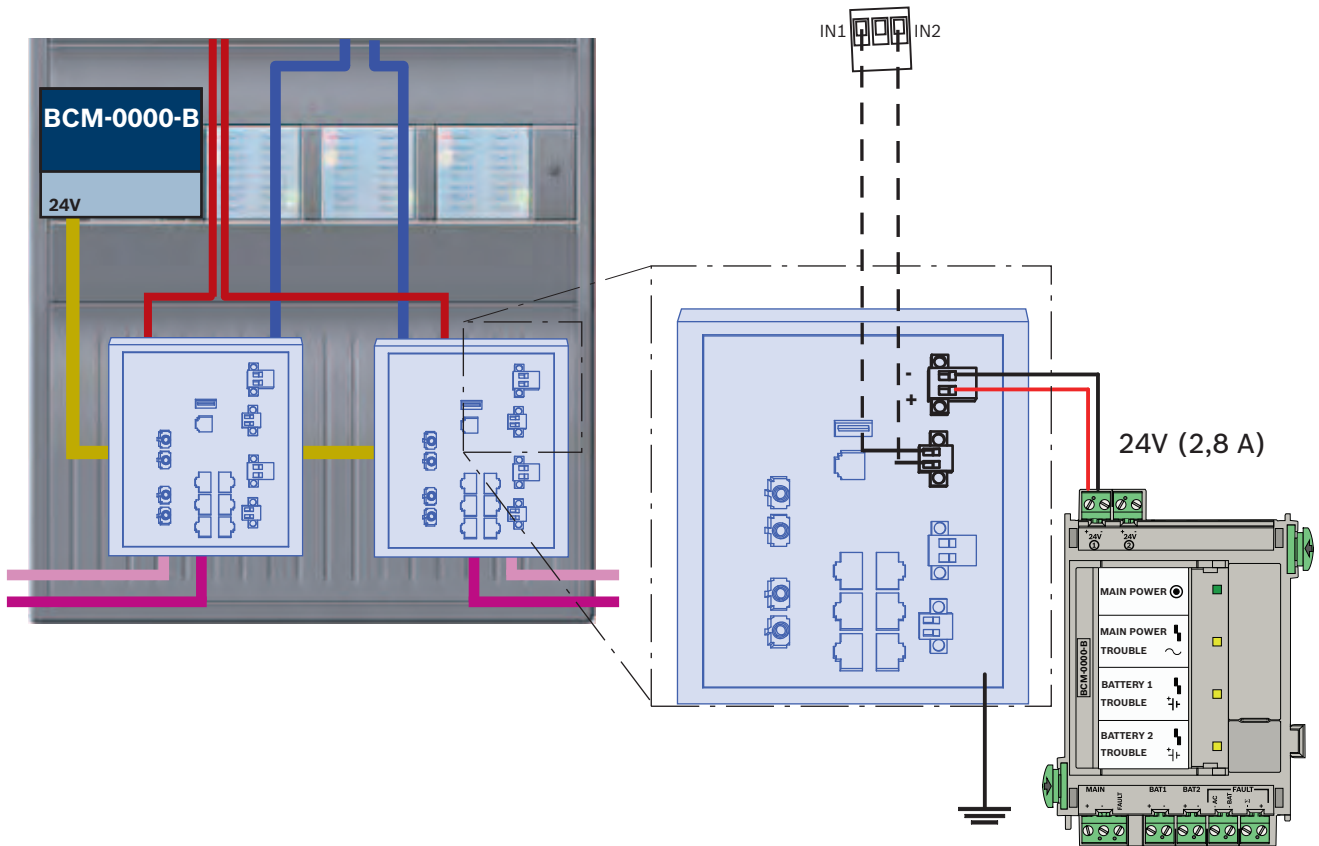






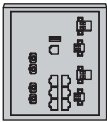
Abbildung 11.2: Anschaltung des Switch an die Stromversorgung und das IOP

Symbol	Beschreibung
	Ethernet-Kabel TX (Kupfer)
	Ethernet-Kabel FX (Lichtwellenleiter)
	24-V-Stromversorgung
	Störungsübertragung
	RSTP-Switch

**Anschaltung von Switches mit Störungsmeldungen an die Eingänge der Zentralensteuerung**



**Abbildung 11.3: Anschluss des Switch an die Stromversorgung und an die Zentralensteuerung**

Symbol	Beschreibung
	Ethernet-Kabel TX (Kupfer)
	Ethernet-Kabel FX (Lichtwellenleiter)
	24-V-Stromversorgung
	Störungsübertragung
	RSTP-Switch



**Hinweis!**

Verwenden Sie zum Anschluss der Switches nicht das mitgelieferte Netzwerkkabel. Verwenden Sie ein Ethernet-Patchkabel, geschirmt CAT5e oder besser.

## 11.3 Abgesetzte Bedieneinheit

Eine abgesetzte Bedieneinheit muss über ein FPP-5000 Externes Netzteil mit Strom versorgt werden. Die Verbindung mit dem Netzwerk wird über 2 Medienkonverter in einem PSS 0002 A oder USF 0000 A hergestellt.

**Hinweis!**

Beachten Sie, dass das FPP-5000 Externe Netzteil und das PSF 0002 A (PSS 0002 A) in unmittelbarer Nähe (ohne Zwischenraum) zur abgesetzten Bedieneinheit montiert werden müssen. Es darf nicht möglich sein, die Anschlusskabel zwischen den Komponenten zu berühren, da sie nicht auf schleichenden Kurzschluss und auf schleichende Unterbrechung überwacht werden.

**Hinweis!**

Verwenden Sie nur Medienkonverter, um eine abgesetzte Bedieneinheit mit einem Ethernet-Zentralennetzwerk zu verbinden.  
Die Verwendung von Switches ist bei der abgesetzten Bedieneinheit nicht zulässig.

**Hinweis!**

Die funktionale Erde der abgesetzten Bedieneinheit muss immer aufgesteckt sein, wenn die Einheit an ein Ethernet-Zentralennetzwerk angeschlossen wird.

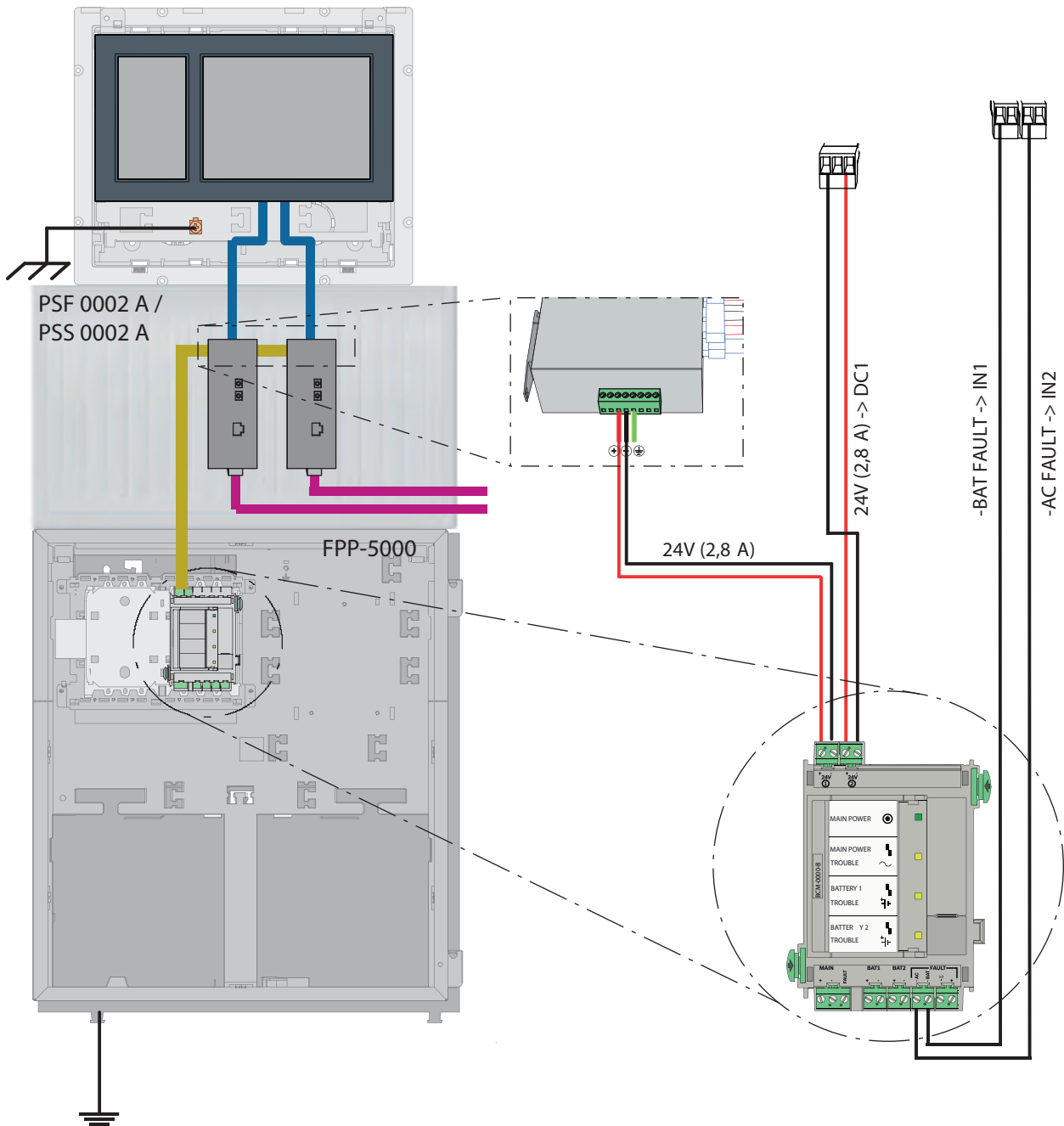






Abbildung 11.4: Verkabelung der abgesetzten Bedieneinheit

Symbol	Beschreibung
	Ethernet-Kabel TX (Kupfer)
	Ethernet-Kabel FX (Lichtwellenleiter)
	24-V-Stromversorgung
	Medienkonverter



## 12 FSP-5000-RPS Einstellungen

Sie können das gesamte Netzwerk mit der RPS-Programmiersoftware über den USB-Port, die Netzwerk-Schnittstelle oder die serielle Schnittstelle der Zentrale programmieren. Um dies zu tun, müssen Sie die Netzwerkeinstellungen der Zentrale konfigurieren und diese neu starten, damit das Netzwerk in Betrieb genommen werden kann.

Alternativ können Sie auch die Netzwerkschnittstelle eines Switches verwenden, der mit diesem Netzwerk verbunden ist.

### 12.1 Netzwerkknoten

Sie müssen das gesamte Netzwerk mit allen FPA-Netzwerkknoten in der FSP-5000-RPS Programmiersoftware programmieren und in das Netzwerk hochladen. Gehen Sie dazu wie folgt vor:

- Verbinden Sie die FPA-Knoten.
  - Stellen Sie die RSN an den einzelnen Knoten ein.
- Passen Sie die Liniennummern der Netzwerkverkabelung so an, dass die geplante Topologie entsteht.
- Überprüfen Sie in der Topologie-Anzeige, ob die Topologie korrekt ist.
- Verbinden Sie bei Bedarf OPC-Server, das Praesideo/PAVIRO-System, UGM-2040-Server und Switches.
- Bearbeiten Sie die Ethernet- und IP-Konfiguration.
  - Vergeben Sie die IP-Adressen oder nutzen Sie die Standardeinstellungen, wenn Sie eine Topologie mit weniger als 20 RSTP-Switches verwenden.
  - Wählen Sie das passende Redundanzprotokoll für die eingestellte Topologie.
- Führen Sie eine Konsistenzprüfung durch.
- Stellen Sie über Ethernet, USB oder die serielle Schnittstelle eine Verbindung mit dem Netzwerk her.
- Führen Sie eine Mehrfachanmeldung durch.
- Führen Sie für jede Zentrale eine komplette Autodetektion durch.
- Fordern Sie die Konfigurationsinformationen an und führen Sie alle Aufgaben durch. Kontrollieren Sie die Fehlermeldungen nach dem Neustart des Zentralennetzwerkes, und beheben Sie eventuell vorhandene Fehler.

### 12.2 Leitungsnummern

Sie müssen jedem im Netzwerk genutzten Anschluss eine Leitungsnummer zuweisen. Es ist nicht relevant, ob dies eine CAN-Verbindung oder eine Ethernet-Verbindung ist.

Es ist möglich, eine Leitungsnummer sowohl für eine CAN-Verbindungen wie auch für eine Ethernet-Verbindung zu verwenden. Um aber eine bessere Übersicht über die Verbindung zu erhalten, sollten Sie unterschiedliche Nummernbereiche verwenden.

Beachten Sie, dass bei Verwendung von **Netzwerk** als **Leitungstyp** im Fenster **Netzwerkschnittstelle** die Leitungsnummer für alle Verbindungen 0 sein muss.

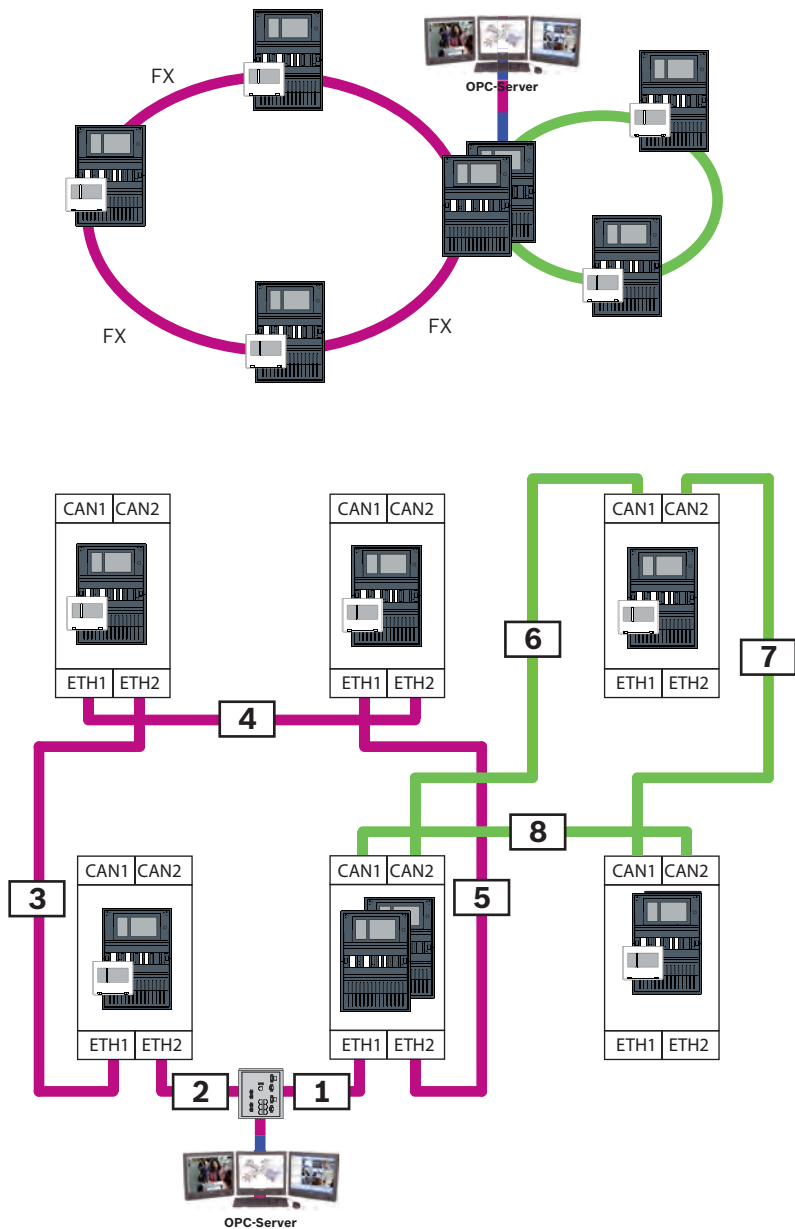


Abbildung 12.1: Beispiel eines Netzwerks und mögliche Leitungsnummerierung

### 12.3 Switches

Wenn Sie Switches in Ihrem Netzwerk verwenden, müssen diese in der FSP-5000-RPS-Programmiersoftware eingefügt werden. Sie können jedem angelegten Switch bis zu 128 Ports zuweisen. Um Ihr Netzwerk zu erstellen, können Sie den einzelnen Ports die verbundenen Leitungsnummern zuweisen.

### 12.4 OPC-Server

OPC-Server in Ihrem Netzwerk müssen zur Programmiersoftware FSP-5000-RPS hinzugefügt werden.

Sie müssen die folgenden Einstellungen in der Software FSP-5000-RPS und beim OPC-Server festlegen:

- Netzwerkknoten
- Netzwerkgruppe
- RSN

- IP-Adresse
- Port

Der OPC-Server verwendet standardmäßig den Port 25000.

**Hinweis!**

EN 54

Die Verbindung eines Gebäudemanagementsystems (z. B. BIS) über eine Ethernet-Schnittstelle mit einem OPC-Server oder FSI-Server ist EN 54-konform, wenn die EN 54-relevanten Funktionen nur von der Brandmelderzentrale ausgeführt werden. Alle EN 54-relevanten Steuerungs- oder Verwaltungsfunktionen (z. B. Steuerung von Signalgebern oder Abschaltungsverwaltung) mit dem Gebäudemanagementsystem erfordern, dass eine individuelle EN 54-Zertifizierung des gesamten Systems von einem Zertifizierungsinstitut vorliegt.

**Hinweis!**

Programmiersoftware FSP-5000-RPS

Sie müssen jedem Netzwerkknoten einen OPC-Server zuweisen, von dem Status übertragen werden soll.

## 12.5

### UGM-2040 Server

**Hinweis!**

Alle Zentralensteuerungen und UGM-Server müssen sich im selben Subnetzwerk befinden und die gleiche Multicast-Adresse haben.

Bei mehreren Zentralenkonfigurationen oder Netzwerken müssen sich diese im selben Subnetzwerk befinden. Die Multicast-Adressen müssen sich unterscheiden.

**Hinweis!**

Sie müssen den UGM-2040-Server jedem Netzwerkknoten zuweisen, von dem Status übertragen werden sollen

Um eine Zentrale mit der UGM-2040 zu verbinden, müssen Sie die physische Struktur des Netzwerks in RPS simulieren. Dazu gehören auch die Liniennummern zwischen der verbindenden Zentralensteuerung und den Switches der UGM-2040.

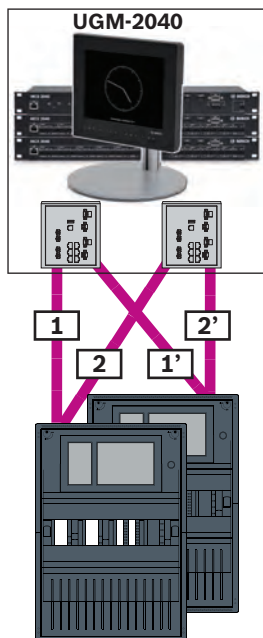


Abbildung 12.2: Beispiel für eine Liniennummerierung für die UGM-2040

# 13 Anhang

## 13.1 Ethernet Fehlermeldungen

Beachten Sie, dass bei einem Fehler jeweils die Fehlermeldung sowie der Gruppenfehler angezeigt werden.

Physikalische Adresse	Logische Adresse	Fehlermeldung	Beschreibung und mögliche Ursache
Gruppenstörungen, die sich auf allgemeine Netzwerkstörungen beziehen			
135.0.1.0	Netzwerk 1.0	<b>Allgemeine Netzwerkstörung</b>	Die Version der Zentralenetzwerksoftware ist nicht kompatibel. Es sind zwei verschiedene Softwareversionen vorhanden.
Gruppenstörungen, die sich auf das Netzwerk beziehen			
135.0.6.1	Netzwerk 2.1	<b>Doppelte IP-Adresse</b>	Eine IP-Adresse wurde zweimal vergeben.
135.0.6.2	Netzwerk 2.2	<b>IP-Einstellungen</b>	Die IP-Konfiguration der meldenden Zentrale unterscheidet sich von der RPS-Konfiguration.
135.0.6.3	Netzwerk 2.3	<b>Redundanzeinstellungen</b>	Die Redundanzkonfiguration (RSTP, RSTP-Parameter, Dual Homing oder nichts) der meldenden Zentrale unterscheidet sich von der RPS-Konfiguration.
Gruppenstörungen, die sich auf das Rapid Spanning Tree Protocol (RSTP) beziehen			
135.0.7.1	Netzwerk 3.1	<b>RSTP-Fallback</b>	Die meldende Zentrale hat vom RSTP-Modus in den STP-Modus (Kompatibilitätsmodus) gewechselt. Es wurde ein STP-Gerät an das Netzwerk angeschlossen.
135.0.7.2	Netzwerk 3.2	<b>RSTP-Topologieänderung</b>	Die RSTP-Netzwerk-Topologie hat sich verändert. Es wurde zum Beispiel ein weiteres RSTP-Gerät im Netzwerk hinzugefügt. Diese Meldung kann auch bei einer Leitungsunterbrechung angezeigt werden.

Physikalische Adresse	Logische Adresse	Fehlermeldung	Beschreibung und mögliche Ursache
135.0.7.3	Netzwerk 3.3	<b>RSTP Link Type Point2Point</b>	Ein RSTP-Port der meldenden Zentrale hat nicht den Status Point-2-Point. Es wurden zum Beispiel an einem RSTP-Port mehrere RSTP-Geräte angeschlossen. Oder an einem RSTP-Port wurde ein weiteres RSTP-Gerät über eine Half-Duplex-Leitung angeschlossen.
Gruppenstörungen, die sich auf die Netzwerkverbindung beziehen			
135.0.5.1	Netzwerkverbindung 1.0	<b>CAN 1 Störung</b>	Die Datenübertragung an CAN-Bus 1 ist eingeschränkt. Mögliche Ursachen sind zum Beispiel: Kabelbrüche, Kabel nicht eingesteckt, Störeinflüsse auf das Kabel.
135.0.5.2	Netzwerkverbindung 2.0	<b>CAN 2 Störung</b>	Die Datenübertragung an CAN-Bus 2 ist eingeschränkt. Mögliche Ursachen sind zum Beispiel: Kabelbrüche, Kabel nicht eingesteckt, Störeinflüsse auf das Kabel.
135.0.5.3	Netzwerkverbindung 3.0	<b>Ethernet 1 Störung</b>	Die Datenübertragung an Ethernet-Leitung 1 ist eingeschränkt. Mögliche Ursachen sind zum Beispiel: Kabelbrüche, Kabel nicht eingesteckt, Störeinflüsse auf das Kabel.
135.0.5.4	Netzwerkverbindung 4.0	<b>Ethernet 2 Störung</b>	Die Datenübertragung an Ethernet-Leitung 2 ist eingeschränkt. Mögliche Ursachen sind zum Beispiel: Kabelbrüche, Kabel nicht eingesteckt, Störeinflüsse auf das Kabel.







**Bosch Sicherheitssysteme GmbH**

Robert-Bosch-Ring 5

85630 Grasbrunn

Germany

**[www.boschsecurity.com](http://www.boschsecurity.com)**

© Bosch Sicherheitssysteme GmbH, 2019