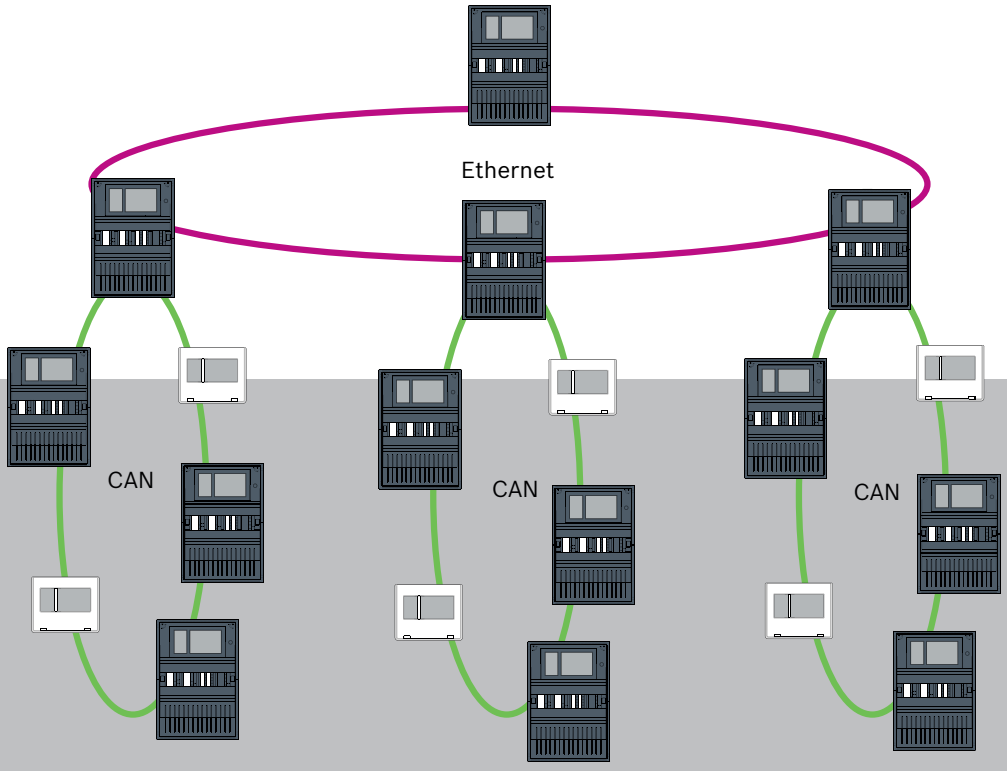
AVENAR panel Serie | FPA-5000 | FPA-1200



de Handbuch Vernetzung

Inhaltsverzeichnis

1	**Sicherheit**	**5**
1.1	Organisatorische Maßnahmen für Rechner mit Service-Clients	5
1.2	Erläuterung der Sicherheitssymbole	6
1.3	Sicherheitshinweise	7
2	**Einführung**	**8**
3	**Systemübersicht**	**9**
4	**Topologien**	**11**
4.1	CAN-Ring	16
4.2	Ethernet-Ring	16
4.3	Ethernet/CAN Doppelring	16
4.4	CAN-Ring mit Ethernet-Segmenten	17
4.5	Ethernet-Backbone mit Sub-Ringen (Ethernet/CAN)	17
4.6	Anschalten von Ethernet-Ringen	18
5	**Ethernet-Netzwerk**	**19**
5.1	Protokolle	20
5.2	Netzwerkdurchmesser	20
5.3	Verwendete Kabel	23
5.4	Erstellen oder Ändern eines Ethernet-Netzwerks	23
6	**CAN-Netzwerk**	**25**
6.1	Erstellen oder Ändern eines CAN-Netzwerks	27
7	**Ethernet- und CAN-Verbindungsmuster**	**27**
7.1	Zentralennetzwerk über Ethernet	29
7.2	Zentralennetzwerk über CAN	29
7.3	Anschließen von Diensten zur Zentrale	30
7.4	Zentralennetzwerk über Ethernet mit redundanten Zentralen	31
7.5	Zentralennetzwerk über CAN mit redundanten Zentralen	31
7.6	Zentralennetzwerk über zwei Ethernet-Ringe	32
7.7	Zentralennetzwerk über zwei Ethernet-Ringe mit redundanten Zentralen	32
7.8	Ethernet- und CAN-Netzwerk mit redundanten Zentralen verbinden	33
7.9	Remote Services mit redundaten Zentralen verbinden	33
7.9.1	Redundantes AVENAR panel	33
7.9.2	Redundante FPA	34
7.10	Services zum Schutz von Menschenleben mit redundanten Zentralen verbinden	35
8	**Remote Services**	**35**
8.1	Voraussetzungen für Remote Services	36
8.1.1	Remote Connect	36
8.1.2	Fire System Explorer	39
8.2	Remote Alert	40
8.3	Remote Maintenance	40
8.4	Remote Maintenance für privates Sicherheitsnetzwerk	41
9	**Sicherheitsmanagement-System (BIS)**	**42**
10	**Smart Safety Link**	**45**
10.1	Eine direkte VAS-Schnittstelle	46
10.1.1	Praesideo und PAVIRO	46
10.1.2	PRAESENSA	47
10.2	Mehrere direkte VAS-Schnittstellen	48
10.3	VAS integriert in Ethernet-Zentralennetzwerk	49
11	**Übergeordnete Zentrale**	**50**

12	**Installation**	**51**
12.1	Einstellungen auf Medienkonvertern	51
12.2	Installieren des Ethernet-Switch	53
12.3	Einstellungen am Switch	53
12.3.1	IP-Adresse vergeben	53
12.3.2	Redundanzeinstellungen programmieren	54
12.3.3	Fehlerrelais programmieren	55
12.3.4	Verbindungsüberwachung programmieren	55
12.3.5	QoS-Priorität	56
12.3.6	IGMP Snooping aktivieren	56
12.4	CAN-Netzwerk	57
13	**Ethernet-Verkabelung**	**62**
13.1	Medienkonverter	63
13.2	Ethernet-Switch	64
13.3	Abgesetzte Bedieneinheit	67
14	**FSP-5000-RPS Einstellungen**	**69**
14.1	Netzwerkknoten	69
14.2	Liniennummern	69
14.3	Switches	70
15	**Anhang**	**70**
15.1	Ethernet Fehlermeldungen	70
	Index	**73**

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!
Eine Warnung weist Sie darauf hin, dass die Gefahr besteht, dass Gegenstände beschädigt werden.

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. Laserdiode der 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.

Vorsicht!
Für den Aufbau eines zentralen Brandmeldenetzwerks 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.

Smart Safety Link

Warnung!
Ethernet-Sicherheitsrisiken
Verbinden Sie PRAESENSA nicht mit FPA-5000/FPA-1200 über Smart Safety Link aufgrund von Ethernet-Sicherheitsrisiken.

Hinweis!
VdS 2540
Das Sprachalarmierungssystem muss bündig mit der Brandmelderzentrale in einem Raum untergebracht sein. Andernfalls sind die Anforderungen von VdS 2540 für Datenübertragungswege nicht erfüllt.

Zentralennetzwerk

Hinweis!
EN 54
Verwenden Sie zum EN 54-konformen Aufbau der Netzwerke nur Komponenten, die für den Einsatz in zentralen Brandmeldenetzwerken 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 – Ethernet-Netzwerk
Bei Ethernet-Zentralennetzwerken ist zu beachten, dass für Installationen in Deutschland, wo die Einhaltung der VdS 2540 gefordert wird, Lichtwellenleiter für alle Datenübertragungswege verwendet werden müssen. Die einzige Ausnahme ist das Innere eines Gehäuses.

Hinweis!
Verwenden Sie für normale Anwendungen die Standard-Netzwerkeinstellungen.
Änderungen an den Standard-Netzwerkeinstellungen dürfen nur versierte Benutzer mit Netzwerkkenntnissen vornehmen.

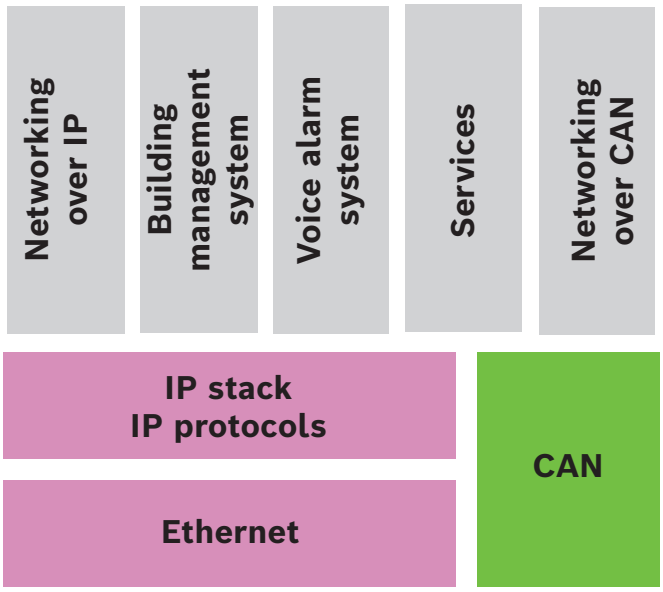
Hinweis!
Anwendbare Topologien
Die Funktionalität und Kommunikation der Zentralen untereinander wird durch den Zentralentyp beschränkt. Informationen zu Diensten, die Anzahl der anschließbaren Zentralen und der anschließbaren abgesetzten Bedieneinheiten finden Sie in den technischen Daten der Zentrale.

2 Einführung

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

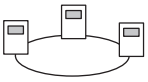
- Vernetzung über TCP/IP
  Aktivieren Sie in FSP-5000-RPS die Kommunikation der Zentralen untereinander im Ethernet-Netzwerk.
- Sicherheitsmanagement-System (BIS)
  Erstellen eines Servers in der FSP-5000-RPS-Konfiguration
- Verbindung zum Sprachalarmierungssystem
  Fügen Sie der FSP-5000-RPS Konfiguration 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.

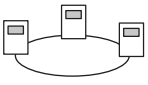
Hinweis!
Ungewollte Datenübertragung
Deaktivieren Sie die Kommunikation der Zentrale über TCP/IP, in FSP-5000-RPS, wenn die Ethernet-Schnittstelle der Zentralensteuerung nur für die Kommunikation mit dem Gebäudemanagementsystem oder für Remote Services genutzt wird. Andernfalls könnten Branddaten ungewollt 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 Bedieneinheit als redundante Zentrale verwenden.	Die redundante Zentralensteuerung kann Standard sein. Sie können auch eine abgesetztes Bedieneinheit als redundante Zentrale verwenden.	Nicht möglich	Nicht möglich

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.
Überprüfen Sie beim Austausch einer abgesetzten Bedieneinheit der FPA Serie durch eine abgesetzte Bedieneinheit der AVENAR panel Serie, ob der Leitungswiderstand innerhalb des für die abgesetzte Bedieneinheit der AVENAR panel Serie angegebenen Bereichs 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!
Firmware-Versionen
Für ein System, das ausschließlich AVENAR-Knoten enthält, wird empfohlen, die neueste Zentralenfirmware 4.x zu verwenden.
Für ein System, das mindestens einen Knoten der FPA-Serie enthält, wird empfohlen, die neueste Zentralenfirmware 3.x zu verwenden.

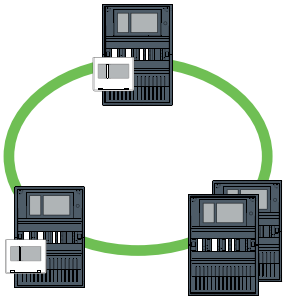
Hinweis!
Vom 1. Januar 2022 bis zum 31. Dezember 2025 befindet sich die Tableau-Firmware-Version 3.x im Wartungsmodus. In diesem Zeitraum werden neue Versionen veröffentlicht, die Korrekturen für kritische Fehler und kritische Sicherheitslücken enthalten. Es sind keine neuen Produktleistungsmerkmale, LSN-Peripheriegeräte, GUI-Sprachen und normativen Änderungen geplant.
Nach dem 31. Dezember 2025 erhöht die Ausführung der Firmware V3.x auf Tableaus, die mit einer Ethernet-Schnittstelle oder einem Netzwerk verbunden sind, die Sicherheitsrisiken. Es wird dringend empfohlen, eine Sicherheitsrisikobewertung durchzuführen. Wenn Sicherheitsrisiken identifiziert werden, ist es zwingend erforderlich, ein Upgrade auf AVENAR panel durchzuführen und die neueste Firmware V4.x auszuführen.

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

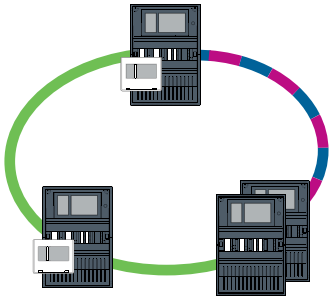
4 Topologien

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

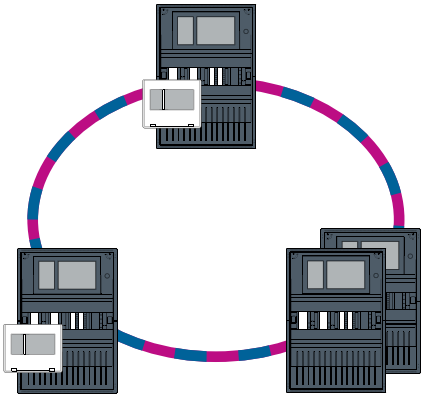
Hinweis!
Anwendbare Topologien
Die Funktionalität und Kommunikation der Zentralen untereinander wird durch den Zentralentyp beschränkt. Informationen zu Diensten, die Anzahl der anschließbaren Zentralen und der anschließbaren abgesetzten Bedieneinheiten finden Sie in den technischen Daten der Zentrale.



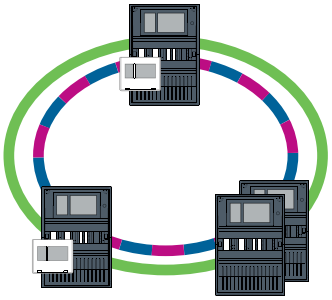
CAN-Ring, Seite 16



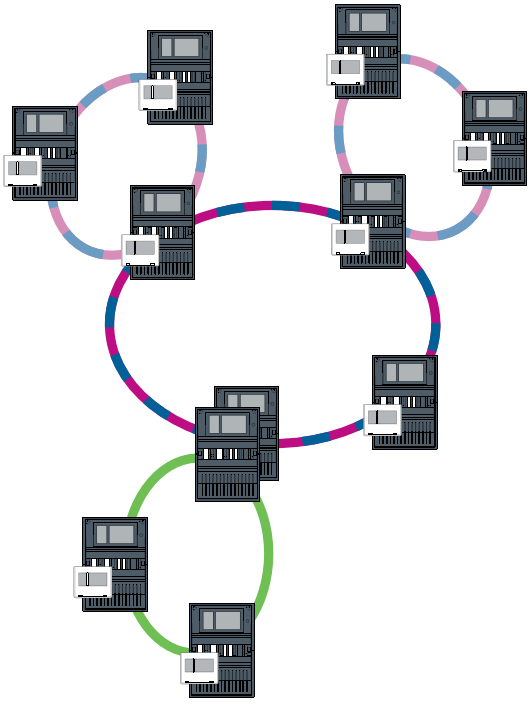
CAN-Ring mit Ethernet-Segmenten, Seite 17



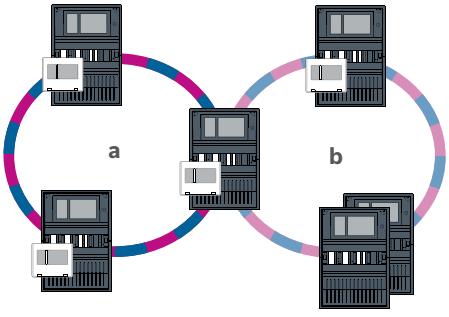
Ethernet-Ring, Seite 16



Ethernet/CAN Doppelring, Seite 16



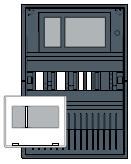
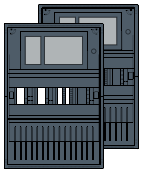
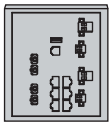
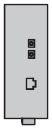
Ethernet-Backbone mit Sub-Ringen (Ethernet/CAN), Seite 17



Anschalten von Ethernet-Ringen, Seite 18

Kabel	Beschreibung
	TX Ethernet-Kabel (Kupfer), Knoten-zu-Knoten-TX-Leitungslänge < 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)
	Zentrale oder redundante Zentrale (in Ethernet-Topologie ein 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
	Sicherheitsmanagement-System (BIS)

Grenzwerte im Netzwerk

Das Netzwerk enthält Knoten.

- Ein Knoten ist entweder eine Zentralensteuerung, eine abgesetzte Bedieneinheit oder ein Server (BACnet-Server, FSI-Server, OPC-Server oder UGM-Server).
- Die Anzahl der Knoten ist auf 32 beschränkt.
- Die Anzahl der logischen Punkte pro Netzwerk ist auf 32768 begrenzt.
- Die Anzahl der logischen Punkte pro Zentrale, die in einem Netzwerk betrieben wird, ist auf 2048 beschränkt.
- Die Anzahl der abgesetzten Bedieneinheiten, die einer Zentrale zugewiesen werden können, ist auf 3 begrenzt.
- Die Anzahl der Server, die einer Zentrale oder abgesetzten Bedieneinheit zugewiesen werden können, ist begrenzt auf:
  - 1 BACnet server
  - 2 FSI server
  - 1 OPC server

– 2 UGM server

Für weitere Informationen sehen Sie sich die im Systemhandbuch angegebenen Systemgrenzwerte an.

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, eine abgesetzte Bedieneinheit oder ein Server 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 Brandmeldenetzwerken 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.

Hinweis!

Anzahl der logischen Punkte

Für eine Standalone-Zentrale können bis zu 4096 logische Punkte angeschlossen werden, auch wenn sie redundant ausgeführt wird. Wenn die Zentrale Teil eines Netzwerks ist, können Sie maximal 2048 logische Punkte 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 20*).

– 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.

4.1 CAN-Ring

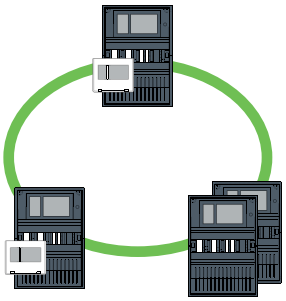


Abbildung 4.1: CAN-Ring

4.2 Ethernet-Ring

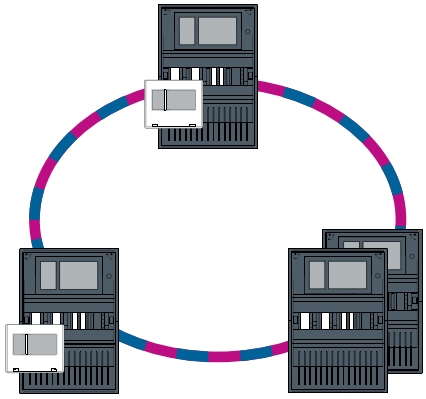


Abbildung 4.2: Ethernet-Ring

4.3 Ethernet/CAN Doppelring

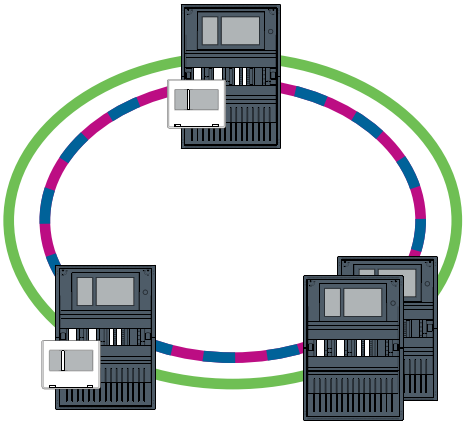


Abbildung 4.3: Doppelter Ring von Ethernet und CAN

4.4 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.

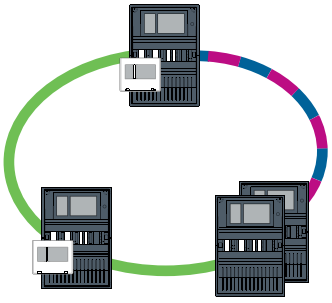


Abbildung 4.4: CAN-Ring mit Ethernet-Segmenten

4.5 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 15*).

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

Hinweis!
Wenn die Zentrale als Schnittstelle zu einem CAN-Sub-Ring dient, muss die Zentrale gemäß EN 54-2 auch dann redundant ausgeführt werden, wenn mehr als 512 Meldepunkte im Sub-Ring angeschlossen sind.
In einem Ethernet-Sub-Ring gilt diese Einschränkung nicht, da die Switches zum Verbinden der zwei 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.

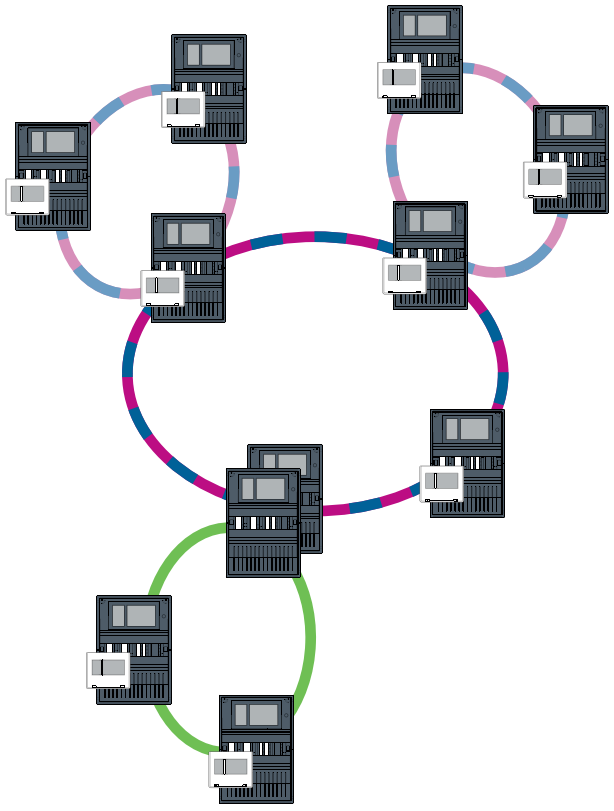


Abbildung 4.5: Ethernet-Backbone mit Sub-Ringen

4.6 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.

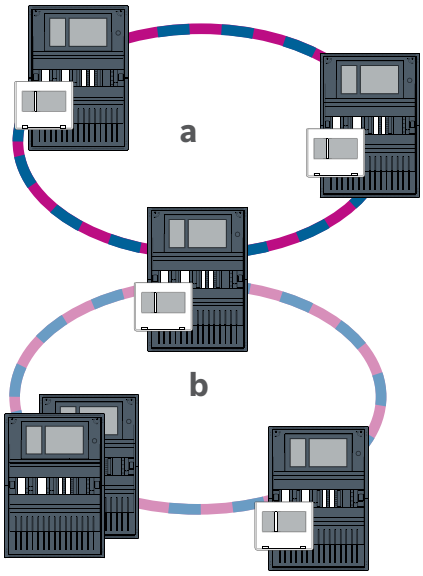


Abbildung 4.6: Anschalten der Ethernet-Ringe über eine nicht redundante Zentrale

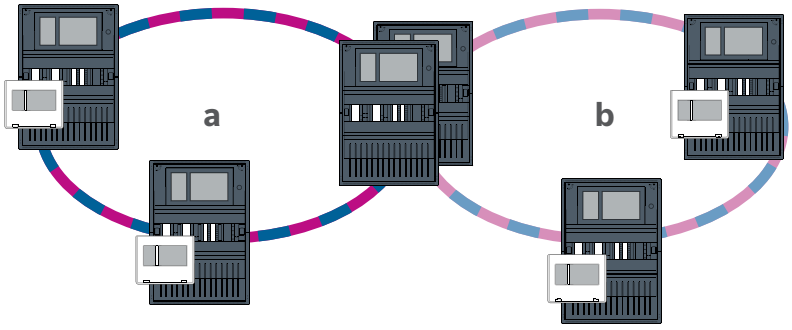


Abbildung 4.7: Anschalten der Ethernet-Ringe über eine redundante Zentrale

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. Zum Anschluss eines Gebäudemanagementsystems, eines Sprachalarmierungssystems oder einer übergeordneten Zentrale 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 eines Gebäudemanagementsystems , eines Sprachalarmierungssystems oder einer übergeordneten Zentrale eingesetzt werden.
4. Wenn es keine Zentralenvernetzung über ETH1 und ETH2 gibt, dann kann jeder für den Anschluss eines Gebäudemanagementsystems, eines Sprachalarmierungssystems oder einer übergeordneten Zentrale verwendet werden.

5.1 Protokolle

SNMP

SNMP wird zur Überwachung und Kontrolle von Netzwerkkomponenten 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 Reperatur automatisch zurückgenommen.

5.2 Netzwerkdurchmesser

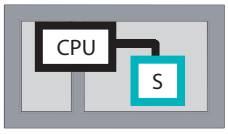
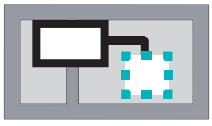
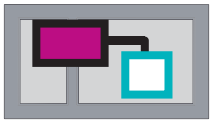
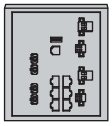
Der Netzwerkdurchmesser des RSTP-Ethernet-Zentralennetzwerks darf nicht größer als 32 sein.

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.
- Gebäudemanagementsysteme 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.

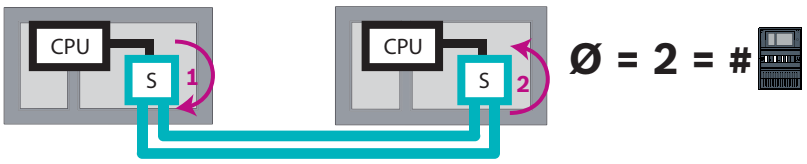


Abbildung 5.1: Netzwerkdurchmesser eines Rings mit zwei Zentralen

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

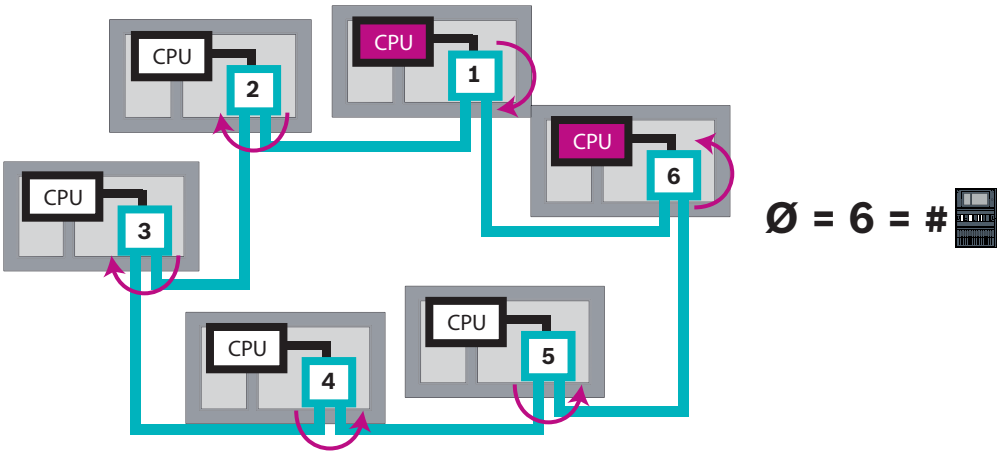


Abbildung 5.2: Netzwerkdurchmesser eines Rings mit sechs Zentralen

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

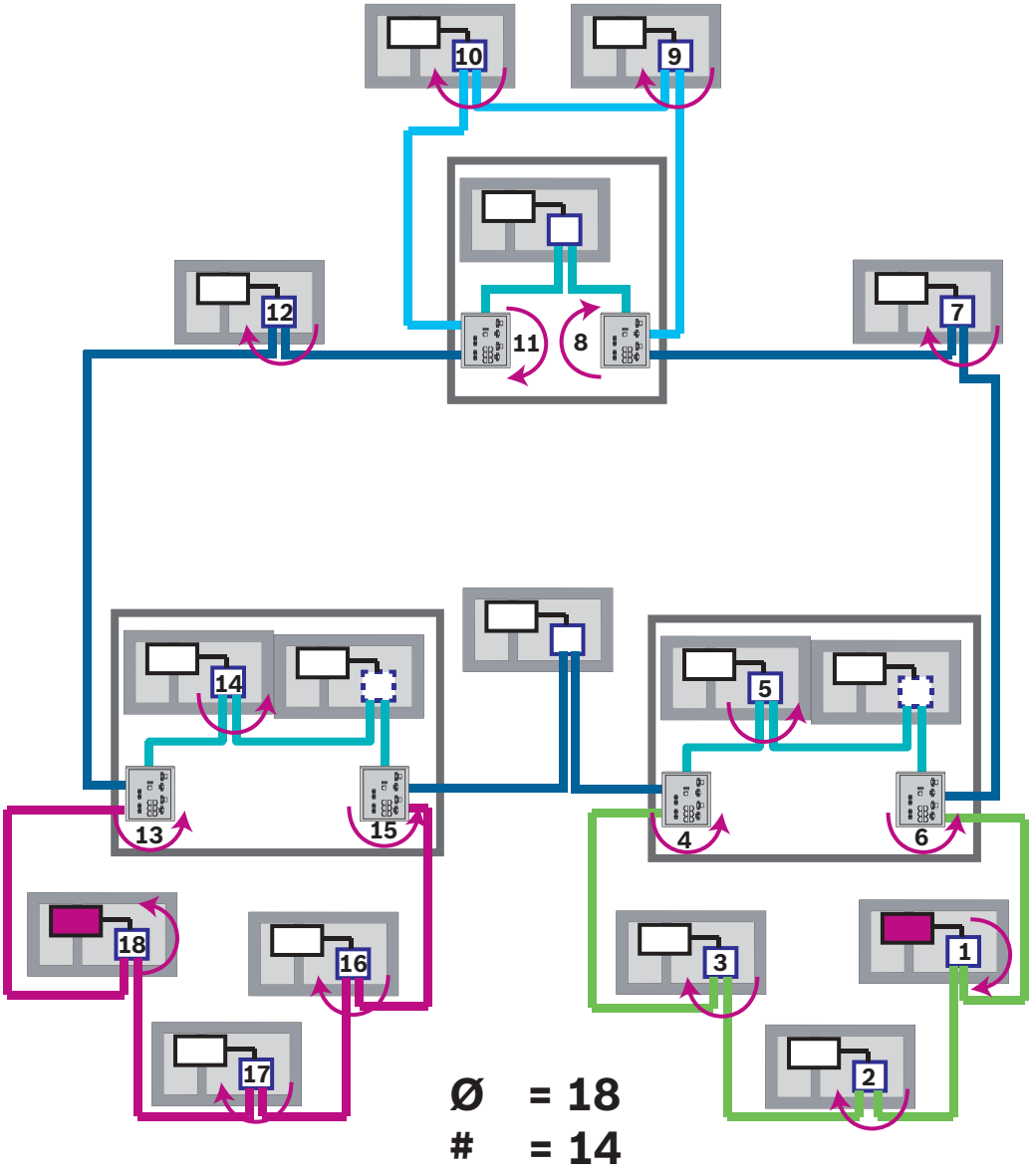


Abbildung 5.3: Netzwerkdurchmesser eines Backbones mit Sub-Ringen

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

5.3 Verwendete Kabel

Verwenden Sie für die Ethernet-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 50/125µ oder Duplex I-VH2G 62.5/125µ, SC-Stecker.
  Single mode: Lichtwellenleiter-Ethernet-Patchkabel, Duplex I-VH2E 9/125µ, 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 – Ethernet-Netzwerk
Bei Ethernet-Zentralennetzwerken ist zu beachten, dass für Installationen in Deutschland, wo die Einhaltung der VdS 2540 gefordert wird, Lichtwellenleiter für alle Datenübertragungswege verwendet werden müssen. Die einzige Ausnahme ist das Innere eines Gehäuses.

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. Zum Anschluss eines Gebäudemanagementsystems, eines Sprachalarmierungssystems oder einer übergeordneten Zentrale 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 eines Gebäudemanagementsystems , eines Sprachalarmierungssystems oder einer übergeordneten Zentrale eingesetzt werden.
4. Wenn es keine Zentralenvernetzung über ETH1 und ETH2 gibt, dann kann jeder für den Anschluss eines Gebäudemanagementsystems, eines Sprachalarmierungssystems oder einer übergeordneten Zentrale 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 Netzwerkkabel 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 zweiadrig (CAN-H und CAN-L). Verbinden Sie CAN-H mit CAN-H und CAN-L mit CAN-L für eine zweiadrige Verbindung. In Ausnahmefällen, z. B. bei hoher EMV-Belastung oder einem großen Unterschied im Erdpotential, kann eine dreiadrige 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 dreiadrige Verbindung. Der Schirmbeidraht des CAN-Kabels wird nur auf einer Seite mit dem Metallgehäuse der Zentrale verbunden.

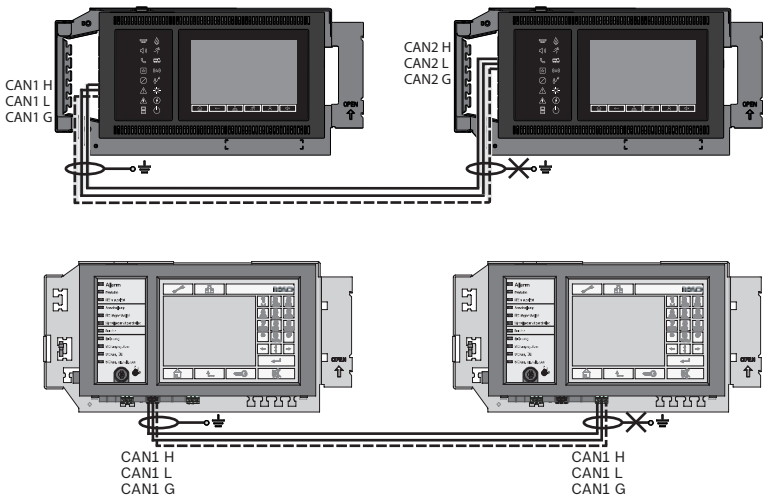


Abbildung 6.1: CAN-Verbindung (oben: AVENAR, unten: FPA)

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.

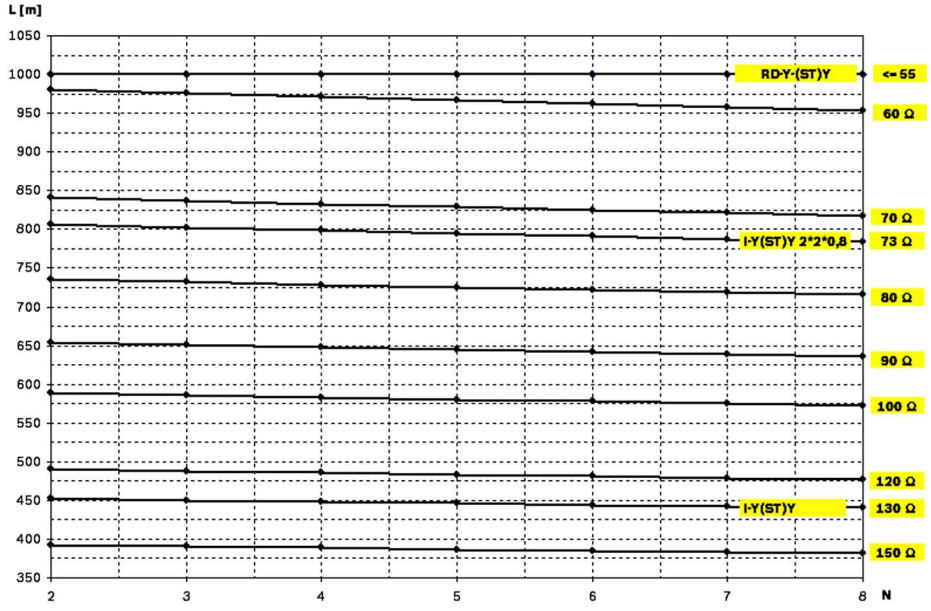


Abbildung 6.2: CAN-Netzwerk: Erreichbare Leitungslänge abhängig von der Anzahl der Knoten und dem Leitungswiderstand

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.

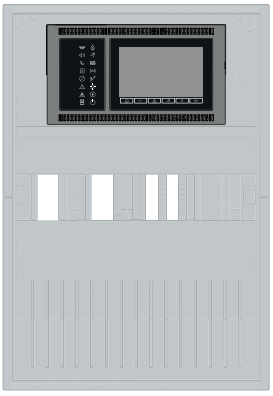
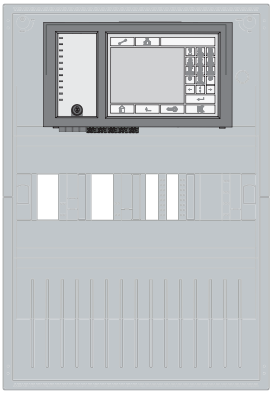
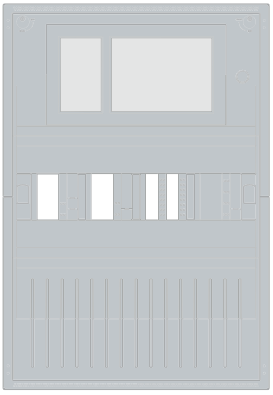
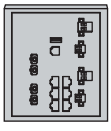
Vorgehen zum Erstellen eines CAN-Netzwerks

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
	TX Ethernet-Kabel (Kupfer), Knoten-zu-Knoten-TX-Leitungslänge < 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 **nicht** 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.

Symbol	Beschreibung
	AVENAR panel
	FPA
	AVENAR panel oder FPA
	Ethernet-Switch als externer RSTP-Switch (im Allgemeinen Ethernet-Switch MM)
	Medienkonverter
	Sicheres Netzwerk-Gateway für Remote Services
	Anschluss an Gebäudemanagementsystem, Sprachalarmierungssystem oder übergeordnete Zentrale

7.1 Zentralennetzwerk über Ethernet

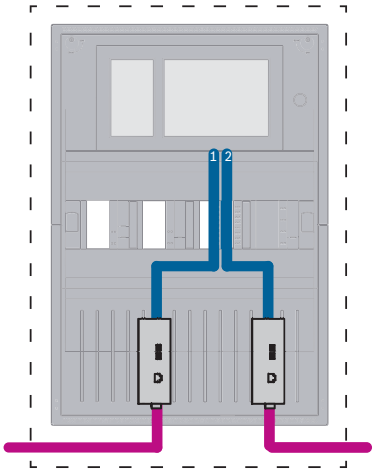


Abbildung 7.1: Zentralennetzwerk über Ethernet

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

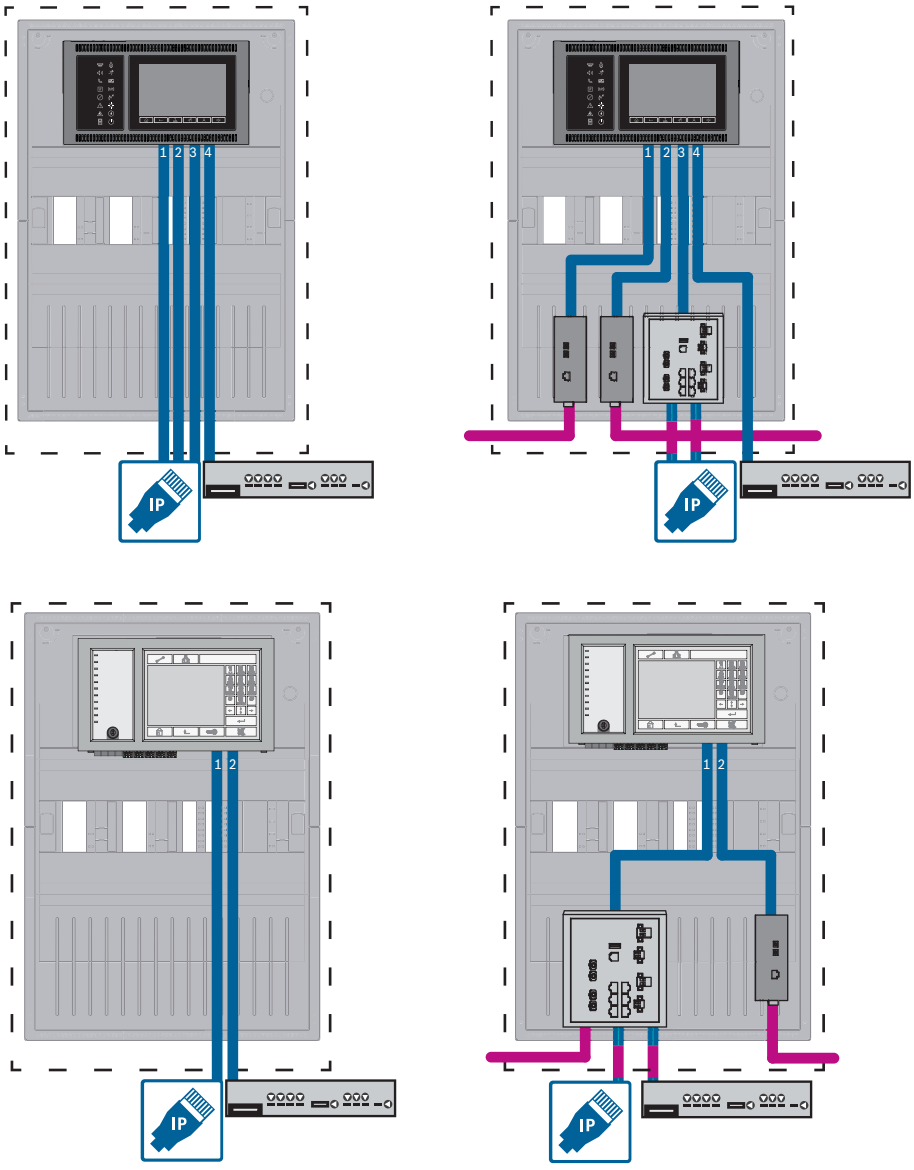


Abbildung 7.3: Links: ohne Zentralennetzwerk, rechts: mit Zentralennetzwerk

Nur wenn mehr als zwei Dienste an die Zentrale angeschlossen sind, ist der Ethernet-Switch erforderlich.

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 Zentralennetzwerk über Ethernet mit redundanten Zentralen

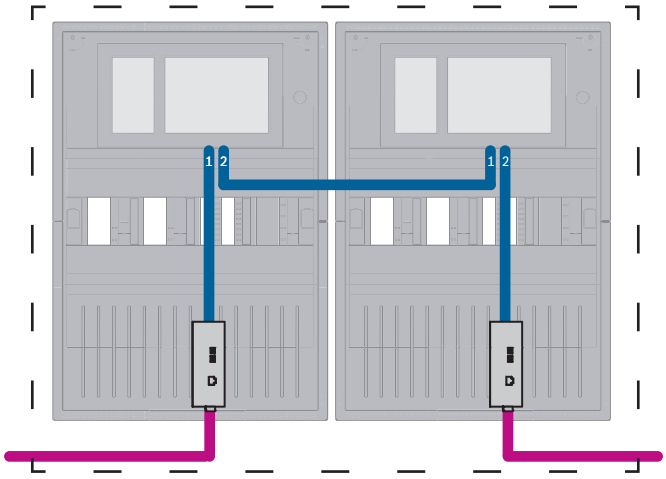


Abbildung 7.4: Zentralennetzwerk über Ethernet mit redundanten Zentralen

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

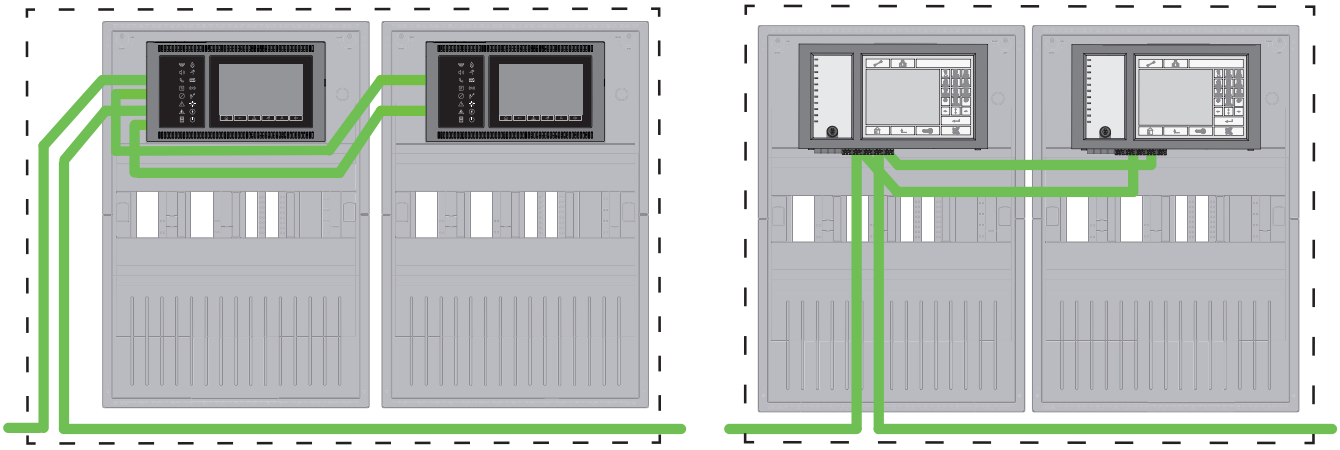


Abbildung 7.5: Zentralennetzwerk über CAN mit redundanten Zentralen

7.6 Zentralennetzwerk über zwei Ethernet-Ringe

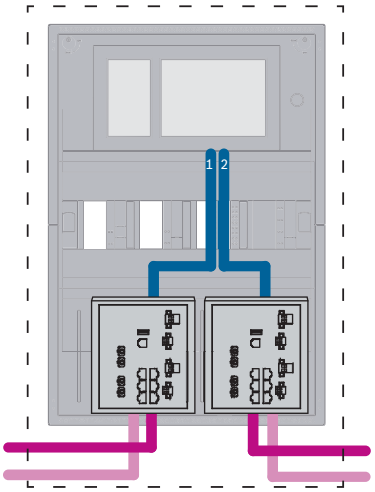


Abbildung 7.6: Ethernet-Netzwerke verbinden

7.7 Zentralennetzwerk über zwei Ethernet-Ringe mit redundanten Zentralen

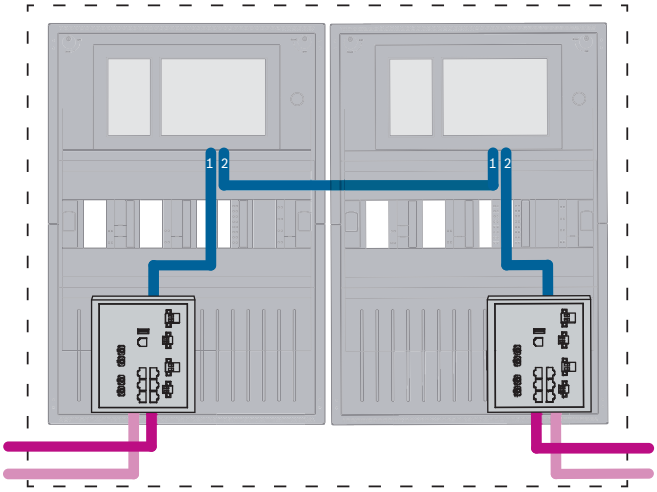


Abbildung 7.7: Ethernet-Netzwerke mit redundanten Zentralen verbinden

7.8 Ethernet- und CAN-Netzwerk mit redundanten Zentralen verbinden

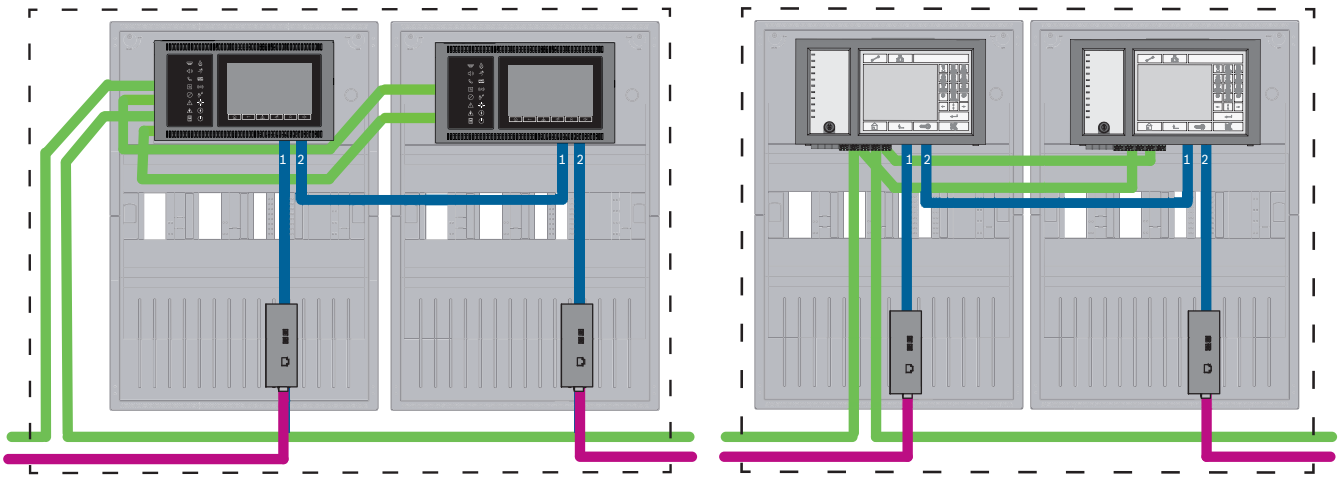


Abbildung 7.8: Ethernet- und CAN-Netzwerk mit redundanten Zentralen verbinden

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 redundaten Zentralen verbinden

Das sichere Netzwerk-Gateway kann an eine redundante FPA oder an ein redundantes AVENAR panel angeschlossen werden. Aus den folgenden Gründen sollten Sie das sichere Netzwerk-Gateway nicht an ein redundantes AVENAR panel sondern an ein AVENAR panel ohne Redundanz anschließen:

- Das Verfahren ist eine Zwischenlösung.
- Im Falle einer Verbindung zu einem Gebäudemanagementsystem muss der ETH3-Port der redundanten Zentralensteuerung verwendet und konfiguriert werden.

7.9.1 Redundantes AVENAR panel

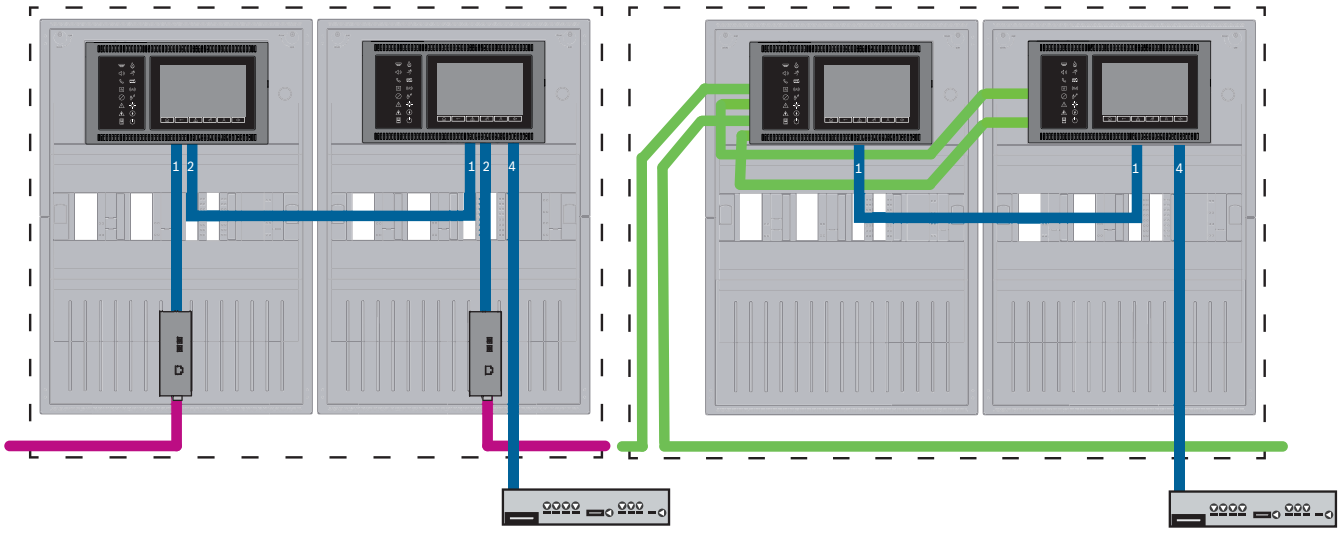


Abbildung 7.9: Links: im Ethernet-Netzwerk Rechts: im CAN-Netzwerk

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

Vorgehensweise

1. Um das sichere Netzwerk-Gateway anzuschließen, verbinden Sie es mit dem ETH4-Port der redundanten Zentralensteuerung.
2. Im CAN-Netzwerk ist ein Ethernet-Kabel vom ETH1-Port zum ETH1-Port der redundanten Zentralensteuerung erforderlich. Konfigurieren Sie die ETH1-Einstellungen im FSP-5000-RPS **Netzwerkschnittstelle**-**Ethernet**-Fenster:
   - Für **Leitungstyp** wählen Sie **Link**
   - Eine Zeilennummer größer als 0 in **Angeschlossen an Kabel Nr** bedeutet, dass die Verbindung überwacht wird.
3. Für beide, CAN-Netzwerk oder Ethernet-Netzwerk, konfigurieren Sie die ETH4-Einstellungen im FSP-5000-RPS **Netzwerkschnittstelle**-**Ethernet**-Fenster:
   - Geben Sie 0 in **Angeschlossen an Kabel Nr** ein.
   - Markieren Sie **Port verwenden**.

7.9.2 Redundante FPA

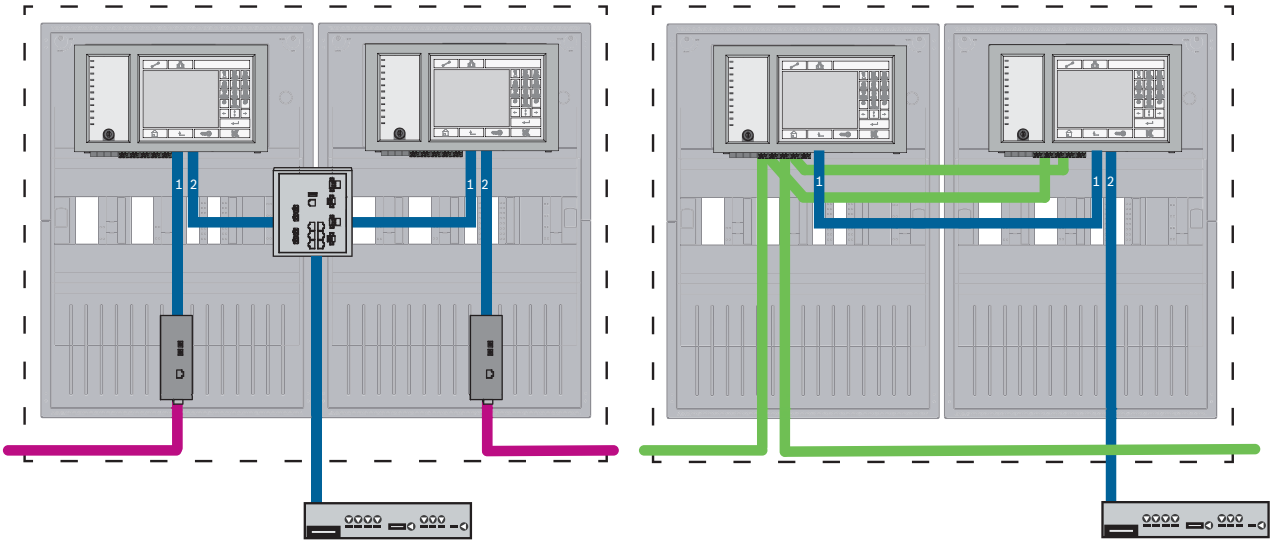


Abbildung 7.10: Links: im Ethernet-Netzwerk Rechts: im CAN-Netzwerk

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

Verfahren im CAN-Netzwerk

1. Um das sichere Netzwerk-Gateway anzuschließen, verbinden Sie es mit dem ETH2-Port der redundanten Zentralensteuerung.
2. Im CAN-Netzwerk ist ein Ethernet-Kabel vom ETH1-Port zum ETH1-Port der redundanten Zentralensteuerung erforderlich. Konfigurieren Sie die ETH1-Einstellungen im FSP-5000-RPS **Netzwerkschnittstelle**-**Ethernet**-Fenster:
   - Für **Leitungstyp** wählen Sie **Link**
   - Eine Zeilennummer größer als 0 in **Angeschlossen an Kabel Nr** bedeutet, dass die Verbindung überwacht wird.
3. Konfigurieren Sie die ETH2-Einstellungen im FSP-5000-RPS **Netzwerkschnittstelle**-**Ethernet**-Fenster:

- Geben Sie 0 in **Angeschlossen an Kabel Nr** ein.
- Markieren Sie **Port verwenden**.

7.10 Services zum Schutz von Menschenleben mit redundanten Zentralen verbinden

Sie müssen Services zum Schutz von Menschenleben an ein AVENAR panel ohne Redundanz anschließen:

- Die Zwischenlösung für Remote Services ist nicht geeignet für Verbindungen zu einem Sprachalarmierungssystem (VAS over IP), das zum Schutz von Menschenleben eingesetzt wird, und auch nicht zu einer übergeordneten Zentrale. Ein EN 54-zertifizierter Switch, der mit der Hauptzentralensteuerung und der redundanten Zentralensteuerung verbunden ist, muss installiert werden.

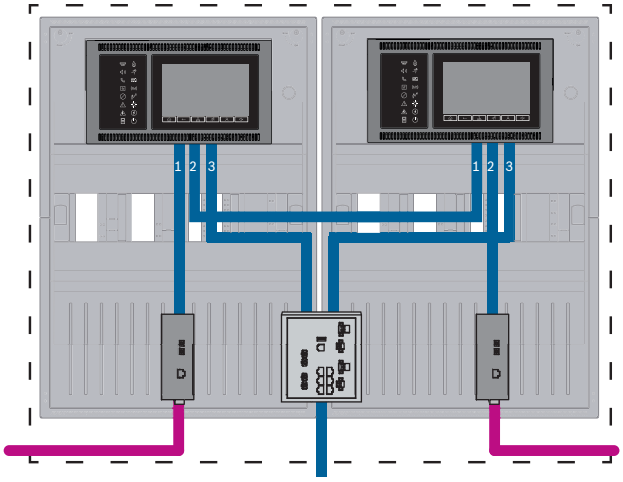


Abbildung 7.11: VAS und übergeordnete Zentrale zu redundantem AVENAR panel

8 Remote Services

Die folgenden Dienste gehören zu Remote Services:

- Remote Alert
- Remote Maintenance

Voraussetzung für Remote Alert und Remote Maintenance ist Remote Connect.

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.

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.

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.

8.1 Voraussetzungen für Remote Services

8.1.1 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. Remote Connect muss in der FSP-5000-RPS Konfiguration dieser Zentrale aktiviert sein.
Die folgenden Topologien zeigen:

- Zentralensteuerungen, die über Ethernet verbunden sind, wobei ein sicheres Netzwerk-Gateway mit dem Netzwerk über einen Ethernet-Switch (im Allgemeinen MM) verbunden ist.
- ein CAN-Netzwerk, bei dem ein sicheres Netzwerk-Gateway mit dem Netzwerk über einen Ethernetport verbunden ist.

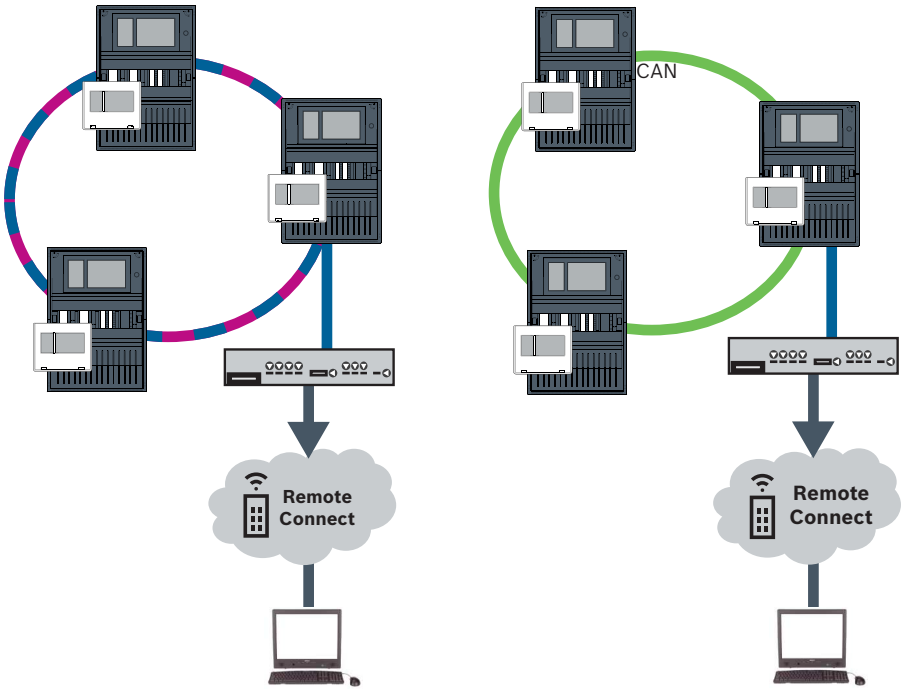


Abbildung 8.1: Remote Connect in einem Ethernet-Ring | Remote Connect in einem CAN-Ring

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.
2. 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

3. 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.
4. 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 hergestellt wurde.
Jede angeschlossene Zentrale oder jedes Zentralennetzwerk hat eine eindeutige System ID.

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

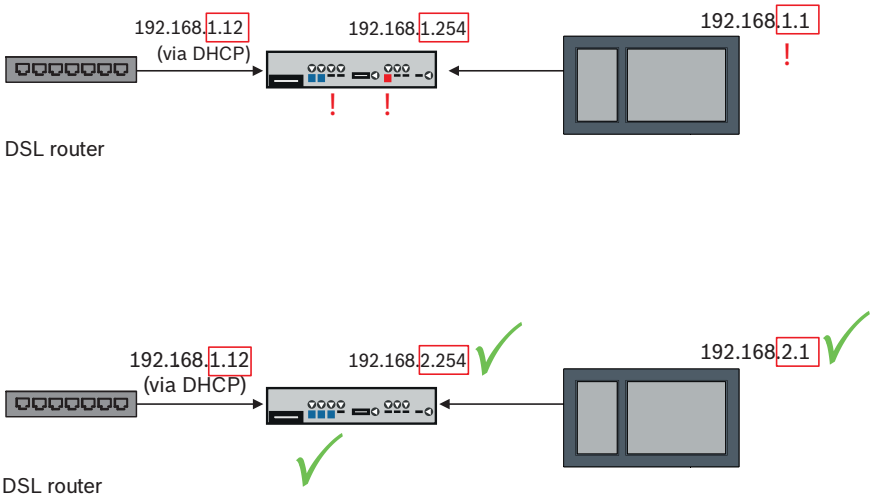
Um zu verhindern, dass EN 54-2-relevanter Multicast-Verkehr an den Router gesendet wird, verwenden Sie den Ethernet-Switch (im Allgemeinen MM, BPA-ESWEX-RSR20), freigegeben mit Zentralenversion 2.8. Aktivieren Sie IGMP Snooping des Ethernet-Switch. Lesen Sie den entsprechenden Abschnitt im Kapitel Installation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

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.



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.

8.1.2 Fire System Explorer

Um Remote Services zu verwenden, müssen Sie einen Fire System Explorer (FSE)-Mandanten haben. Die eindeutige Remote ID repräsentiert Ihr Unternehmen.

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 5.12.28 oder höher und Internetzugang

FSE verwendet SingleKey ID. Weitere Informationen finden Sie auf der SingleKey ID-Seite: https://singlekey-id.com

FSE-Mandant erstellen
Wenn Sie keinen bestehenden FSE-Mandanten verwenden können, müssen Sie einen erstellen unter: https://fse.bosch-nexospace.com/login/
Möglicherweise müssen Sie sich auf der SingleKey ID-Seite anmelden oder registrieren.

Gegebenenfalls müssen Sie die Vertragsbedingungen und die Datenschutzbedingungen akzeptieren.
FSE sendet Ihnen eine E-Mail mit einem Aktivierungslink an die angegebene Adresse.

Anmelden bei einem vorhandenen FSE-Mandanten
Sie haben eine Einladungs-E-Mail erhalten.
1. Klicken Sie auf den Aktivierungslink in der Einladungs-E-Mail.
2. Wählen Sie den Mandanten aus, bei dem Sie sich anmelden möchten. Die Systeme des Mandanten werden angezeigt.

Mit FSP-5000-RPS verbinden
Für die Verbindung zu FSP-5000-RPS müssen Sie ein Zugriffstoken erstellen.
1. Klicken Sie in FSE auf Ihren Benutzernamen, und wählen Sie **Create Access Token** (Zugriffstoken erstellen) aus.
2. Starten Sie FSP-5000-RPS.
3. Klicken Sie auf das Einstellungssymbol, und wählen Sie **Options** (Optionen) aus.
4. Wählen Sie im Fenster **Settings** (Einstellungen) **Remote Services** (Remote Services) aus.
5. Geben Sie unter **Account** (Konto) Ihre FSE-E-Mail-Adresse und Ihr FSE-Passwort ein. Klicken Sie auf **OK**, um fortzufahren.
6. Wählen Sie im Fenster **Configurations** (Konfigurationen) Ihr System aus.
7. Wählen Sie in der Navigationsstruktur **Remote Services** (Remote Services) aus.
8. Wählen Sie **Remote Portal/Fire System Explorer** (Remote Portal/Fire System Explorer) aus der Dropdown-Liste **Access Type** (Zugriffstyp) aus.
9. Kopieren Sie das generierte Zugriffstoken:

– in **User token** (Benutzertoken), wenn Sie an Ihrem PC arbeiten,
– andernfalls in **One time token** (Einmaliges Token).

8.2 Remote Alert

Über Remote Alert übermittelt eine Zentrale relevante Statusinformationen.
Übertragene Daten werden mit Remote Alert analysiert. Bei einem unerwarteten Ereignis wird der Benutzer per E-Mail über den Erhalt von Alarmmeldungen benachrichtigt.
Remote Alert ist auch für Private Secure Network verfügbar.
Ein Teil von Remote Alert ist die **Remote Fire Safety**-Anwendung. Die App ermöglicht es Benutzern, bei Alarmen oder Systemwarnungen umgehend Push-Benachrichtigungen auf ihr Mobilgerät zu erhalten.
Der Benutzer kann auch auf frühere Benachrichtigungen zugreifen, die per E-Mail oder Messenger-Dienst geteilt werden können.
Darüber hinaus bietet die App Updates zum Systemstatus, einschließlich Systemzustand, Konnektivität, Lizenzgültigkeit und ob ein Firmware-Update für die BMZ erforderlich ist.
Die App kann kostenlos heruntergeladen werden: https://play.google.com/store/apps/details?id=com.bosch.remote_fire_safety&gl=EN oder https://apps.apple.com/de/app/remote-fire-safety/id1557422840

8.3 Remote Maintenance

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

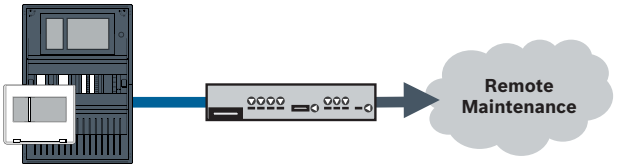


Abbildung 8.2: Remote Maintenance

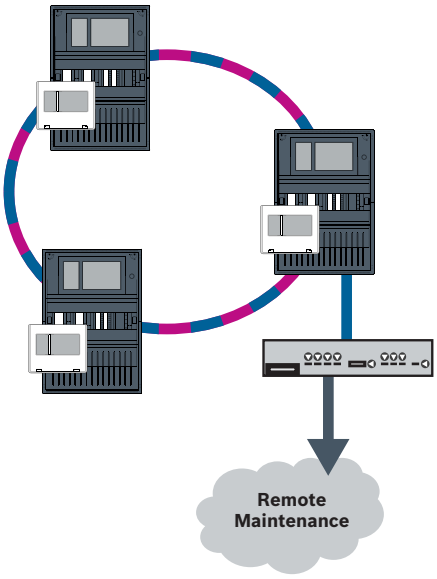


Abbildung 8.3: Remote Maintenance

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 erfasst Daten von relevanten LSN-Geräten und Funktionsmodulen. Die Daten werden für Wartungsaktivitäten analysiert und visualisiert.

8.4 Remote Maintenance für privates Sicherheitsnetzwerk

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

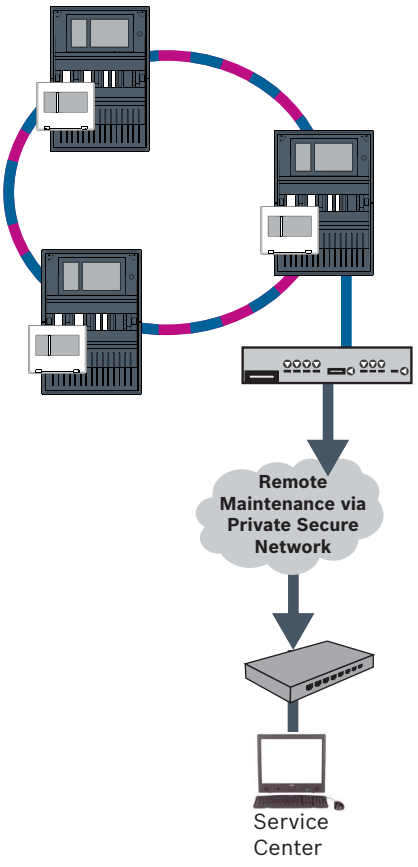


Abbildung 8.4: Remote Maintenance für privates Sicherheitsnetzwerk

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 53*). 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.

9 Sicherheitsmanagement-System (BIS)

Die mit einer Premium-Lizenz ausgestattete Zentralensteuerung kann über eine Ethernet-Schnittstelle und einen der folgenden Server mit einem Gebäudemanagementsystem verbunden werden:

- FSI-Server: FSI (Fire System Interface) ist ein proprietäres Kommunikationsprotokoll von Bosch. Für eine maßgeschneiderte Integration steht ein Software Development Kit (SDK) zur Verfügung.
- OPC-Server: OPC (OLE for Process Control) ist ein mit dem Building Integration System (BIS) kompatibles, standardisiertes Kommunikationsprotokoll.
- BACnet-Server: BACnet (Building Automation and Control Network) ist ein standardisiertes Kommunikationsprotokoll speziell für die Verbindung mit einem Gebäudemanagementsystem eines Drittanbieters.

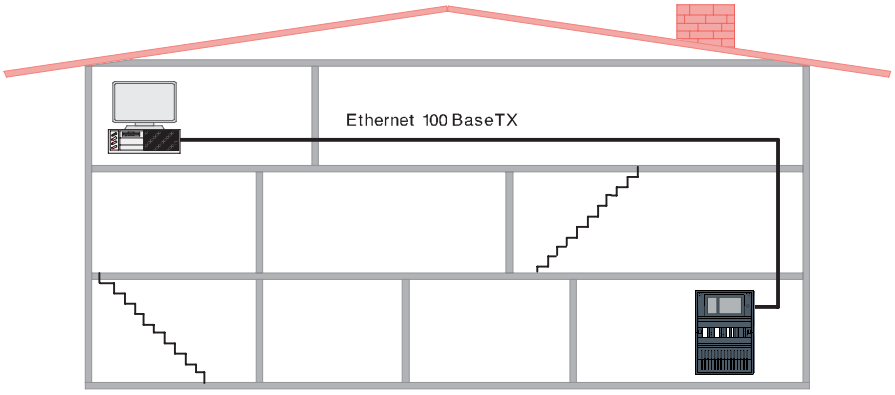


Abbildung 9.1: Anschließen an ein Gebäudemanagementsystem

Bei Anschluss an ein Gebäudemanagementsystem mit 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

Hinweis!
Beachten Sie beim Anschließen des Gebäudemanagementsystems die Sicherheitshinweise unter *Sicherheit, Seite 5*.

Konfiguration in FSP-5000-RPS

Ein Server (OPC server, BACnet server, FSI server) muss in der Programmiersoftware FSP-5000-RPS erstellt werden, um eine Verbindung zu einem Gebäudemanagementsystem herzustellen.

Sie müssen die folgenden Einstellungen sowohl in der Software FSP-5000-RPS als auch auf dem Server vornehmen: Programmieren Sie die logische Knotenadresse (**Netzwerkgruppe** und **Netzwerkknoten-ID**), die physikalische Knotenadresse (**PNA/RSN**) und die IP-Einstellungen (**IP-Adresse** und **Port**).

Bosch empfiehlt, Port 25000 für einen OPC-Server und Port 25001 für einen BACnet server oder einen FSI server zu verwenden.

Sie müssen jeder Zentrale oder abgesetzten Bedieneinheit einen Server zuweisen, von dem Status übertragen werden sollen. Die Anzahl der Server, die einer Zentrale oder abgesetzten Bedieneinheit zugewiesen werden können, ist begrenzt auf:

- 1 BACnet server
- 2 FSI server
- 1 OPC server
- 2 UGM server

Hinweis!
EN 54
Die Verbindung eines Gebäudemanagementsystem mit einer Ethernet-Schnittstelle ist EN 54-konform, wenn die EN 54-relevanten Funktionen nur von der BMZ ausgeführt werden. Alle EN 54-relevanten Steuerungs- oder Verwaltungsfunktionen mit dem Building Management System (z. B. Steuerung von Signalgebern oder Abschaltungsverwaltung) erfordern, dass eine individuelle EN 54-Zertifizierung des gesamten Systems von einem Zertifizierungsinstitut vorliegt.

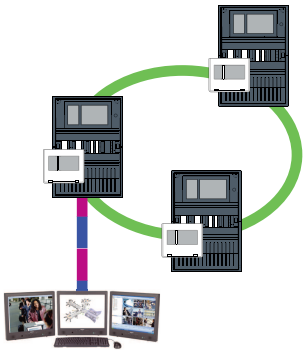
Der Ethernet-Switch zur Anbindung eines Gebäudemanagementsystems muss separat programmiert werden.
Programmieren Sie die IP-Adresse und die Redundanzeinstellungen des Ethernet-Switch (siehe *Einstellungen am Switch, Seite 53*). Da der Switch in unmittelbarer Nähe (ohne Zwischenraum) installiert ist, 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.

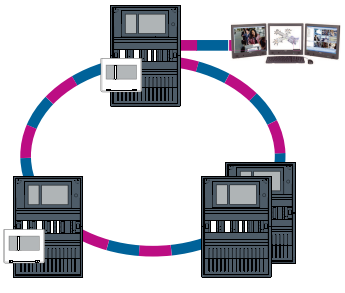
Switches für den Anschluss des Gebäudemanagementsystems und des zweiten Rings müssen separat programmiert werden
Programmieren Sie die IP-Adresse und die Redundanzeinstellungen des Ethernet-Switch (siehe *Einstellungen am Switch, Seite 53*). Für diese Topologie müssen die Störungsausgänge nur verwendet werden, wenn Sie die Stromversorgung des Switch redundant ausgeführt haben (siehe *Ethernet-Switch, Seite 64*).
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.

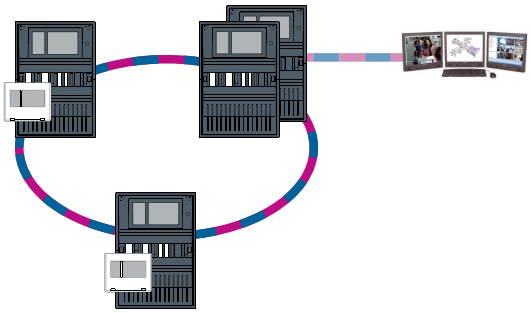
Der Server muss separat programmiert werden
Programmieren Sie die logische Knotenadresse (**Netzwerkgruppe** und **Netzwerkknoten-ID**), die physikalische Knotenadresse (**PNA/RSN**) und die IP-Einstellungen (**IP-Adresse** und **Port**).
Bosch empfiehlt, den Port 25000 für die Ethernet-Schnittstelle zwischen BMZ und Server zu verwenden.
Stellen Sie sicher, dass die Einstellungen in der Programmiersoftware FSP-5000-RPS und im Server identisch sind.

Hinweis!
Weitere Informationen zur Montage und Konfiguration des BACnet- oder OPC-Servers finden Sie im entsprechenden Handbuch im Onlinekatalog unter www.boschsecurity.com. Das Handbuch des FSI-Servers finden Sie im extranet (Zugriffsrechte erforderlich).

Topologien mit Gebäudemanagementsystem
Das Gebäudemanagementsystem kann über ein Ethernet-Kabel (Kupfer) oder einen Lichtwellenleiter angeschlossen werden.

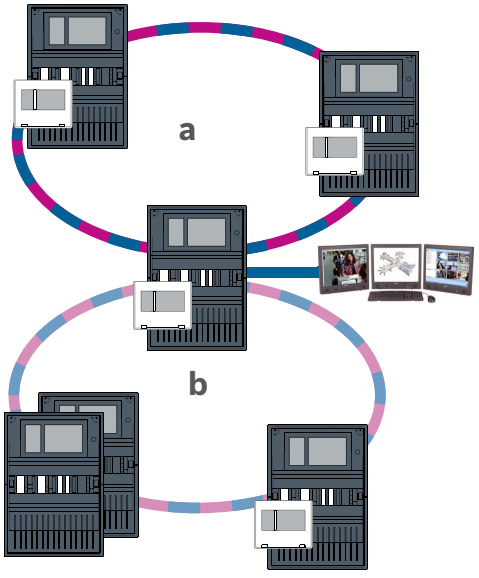

CAN-Ring mit Gebäudemanagementsystem


Ethernet-Ring mit Gebäudemanagementsystem

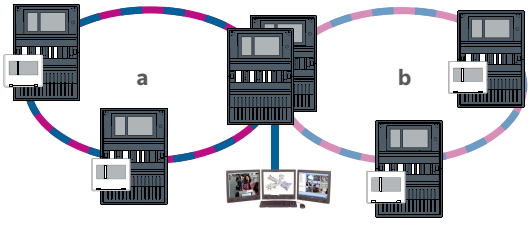


Ethernet-Ring mit Gebäudemanagementsystem zu redundanter Zentrale

In den folgenden Topologien ist Ring a der Backbone. Ring b ist der Sub-Ring.



Anschalten des Ethernet-Rings über eine nicht redundante Zentrale



Anschalten des Ethernet-Rings über eine redundante Zentrale

10 Smart Safety Link

Dieses Kapitel spezifiziert die technische Lösung für eine sichere Ethernet-Schnittstelle zwischen Bosch-Brandmelderzentralen und Bosch-Sprachalarmierungssystemen.
Smart Safety Linkist die zuverlässigste und sicherste Schnittstelle, um ein Brandmelde- und ein Sprachalarmierungssystem (VAS) zu kombinieren. Smart Safety Link bietet außergewöhnliche Flexibilität und Erweiterungsmöglichkeiten.
Der bidirektionale Datenaustausch stellt eine überwachte Verbindung zwischen der BMZ und dem VAS her. Sowohl die BMZ als auch das VAS zeigen eine Störungsmeldung an, wenn die Verbindung unterbrochen wird. Im Falle einer unterbrochenen Verbindung kann der Benutzer die Evakuierung des gesamten Gebäudes manuell starten, indem er eine Sprechstelle des VAS verwendet. Eine Unterbrechung der Schnittstelle führt nicht zu einer automatischen Evakuierung des Gebäudes. Wenn die Schnittstelle wiederhergestellt ist, synchronisiert die BMZ automatisch den aktuellen Alarmstatus mit dem VAS. Im Falle eines

Brandes kann die BMZ automatisch Sprachdurchsagen starten, indem sie virtuelle VAS Auslöser verwenden, die durch Regeln aktiviert werden, die in FSP-5000-RPS konfiguriert werden. Die BMZ erzeugt eine Überwachungsmeldung, wenn ein Evakuierungsereignis von der VAS aus gestartet wird. Eine Störung des VAS erzeugt eine Störungsmeldung auf der Bedieneroberfläche der BMZ.
Über die graphische Bedieneroberfläche des AVENAR panel hat der Bediener die Möglichkeit, die Durchsagen der Brandmelderzentrale stumm zu schalten. Der Bediener kann eine Statusübersicht über alle virtuellen Auslöser anfordern. Jeder virtuelle Auslöser kann mit einer eindeutigen Kennzeichnung versehen werden, die den Ort und die Meldungsart enthält. Eine deutlich unterscheidbare Farbe spiegelt den Zustand jedes virtuellen Auslösers wider. Ein Bediener mit L2-Benutzerrechten kann die Sprachansage im ausgewählten virtuellen Auslöser manuell starten und stoppen.
PAVIRO oder Praesideo kann verbunden werden mit FPA und AVENAR panel.
Aufgrund seiner vernetzten Topologie erfordert PRAESENSA eine Schnittstelle mit verschlüsseltem Datenaustausch. Verwenden Sie ein AVENAR panel mit Zentralenfirmware 4.x zur Verbindung mit PRAESENSA.
Smart Safety Link über Ethernet wurde mit der Firmware 2.11 und FSP-5000-RPS-Version 4.3 eingeführt.

Warnung!
Ethernet-Sicherheitsrisiken
Verbinden Sie PRAESENSA nicht mit FPA-5000/FPA-1200 über Smart Safety Link aufgrund von Ethernet-Sicherheitsrisiken.

Hinweis!
Sprachalarmierungssystem an AVENAR panel angeschlossen
Jede BMZ, die physisch mit einem Sprachalarmierungssystem über Smart Safety Link verbunden ist, benötigt eine Premium-Lizenz.

Hinweis!
Mit FPA verbundenes Sprachalarmierungssystem
Jede Brandmelderzentrale, die physisch mit einem Sprachalarmierungssystem über Smart Safety Link verbunden ist und mit der Firmware-Version 3.x läuft, benötigt keinen Lizenzschlüssel für Sprachalarm.

10.1 Eine direkte VAS-Schnittstelle

Die Brandmelderzentrale und das Sprachalarmierungssystem können über ein einziges TX-Ethernet-Kabel verbunden werden.

Hinweis!
VdS 2540
Das Sprachalarmierungssystem muss bündig mit der Brandmelderzentrale in einem Raum untergebracht sein. Andernfalls sind die Anforderungen von VdS 2540 für Datenübertragungswege nicht erfüllt.

10.1.1 Praesideo und PAVIRO

AVENAR panel und FPA können direkt an den dedizierten Ethernet-Port der Systemsteuerung von Praesideo (PRS-NCO-3) oder PAVIRO (PVA-4CR12) verbunden werden.
Verwenden Sie die offene Schnittstelle für eine Zentrale oder für ein Zentralennetzwerk.

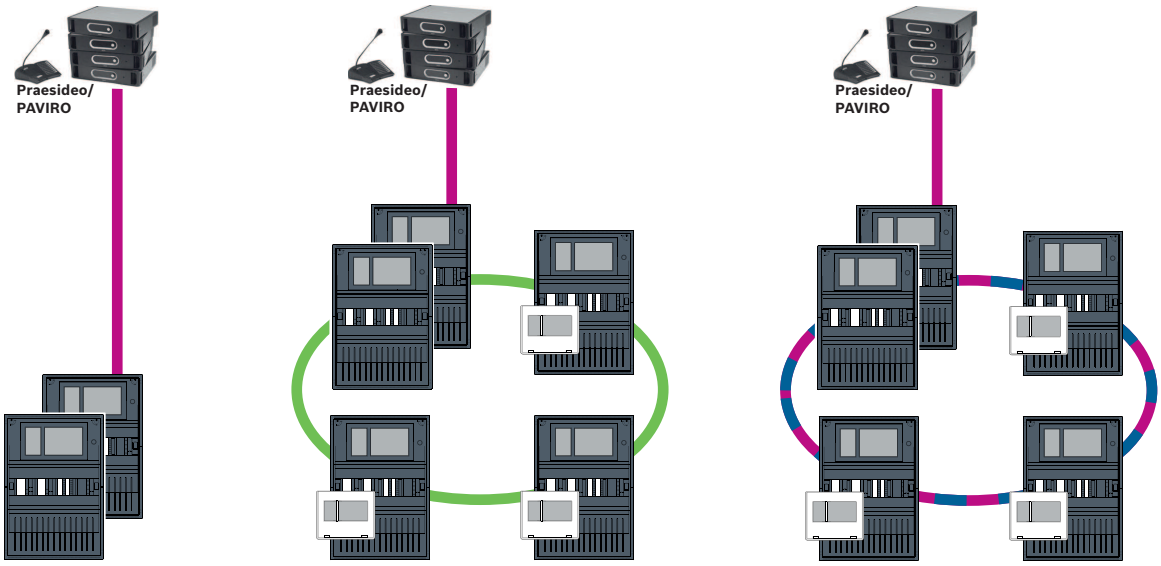


Abbildung 10.1: Eine direkte Praesideo|PAVIRO Schnittstelle

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.

10.1.2 PRAESENSA

PRAESENSA ist ein netzwerkfähiges Sprachalarmierungssystem, das ein IP-Netzwerk für Audio und Steuerung nutzt.
AVENAR panel verbinden Sie immer über einen PRA-ES8P2S Ethernet-Switch, 8xPoE, 2xSFP mit PRAESENSA.

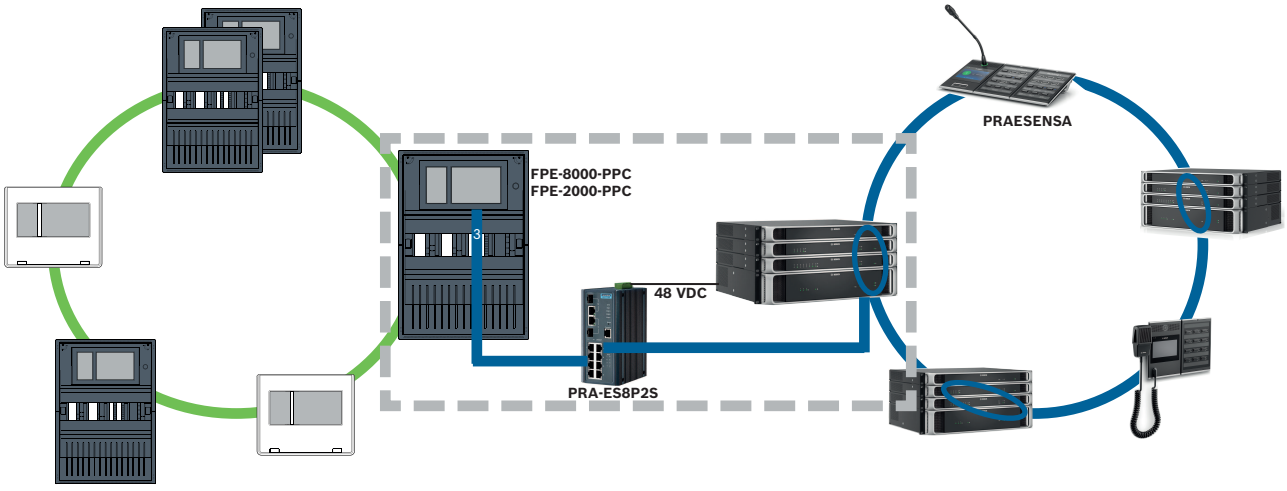


Abbildung 10.2: PRAESENSA an AVENAR panel

Vorsicht!
Ethernet-Sicherheitsrisiken
Verwenden Sie nicht Smart Safety Link zum verbinden von PRAESENSA mit FPA-5000/FPA-1200. Verwenden Sie nur AVENAR panel und AVENAR keypad 8000 im gesamten Netzwerk. Für die Verbindung von PRAESENSA mit FPA-5000/FPA-1200 verwenden Sie Relaiskontakte wie in TI2363/2021 angegeben. Andernfalls entstehen Ethernet-Sicherheitsrisiken.

Hinweis!
PRAESENSA an AVENAR panel
- Verwenden Sie PRA-ES8P2S ausschließlich für Smart Safety Link. Schließen Sie außer PRA-SCL keine anderen PRAESENSA-Geräte an die Ethernet-Ports des Ethernet-Switch, 8xPoE, 2xSFP an. Verwenden Sie den Ethernet-Switch, 8xPoE, 2xSFP nicht für die Verbindung mit einem Gebäudemanagementsystem, einer übergeordneten Zentrale, einem sicheren Netzwerk-Gateway für Remote Services usw.
- Verwenden Sie eine Zentrale mit lediglich einer Zentralensteuerung für die Verbindung mit PRAESENSA mittels Smart Safety Link. Smart Safety Link mit PRAESENSA ist noch nicht mit Zentralenredundanz kompatibel. Die Zentralen im Netzwerk, die nicht direkt mit PRAESENSA verbunden sind, können redundante Zentralensteuerungen haben.
- Verwenden Sie die CAN-Bus-Topologie für das Zentralennetzwerk. Verwenden Sie kein Ethernet-Zentralennetzwerk.
- Alle AVENAR panel und alle AVENAR keypad 8000 im Netzwerk müssen mit Zentralenfirmware 4.x laufen.

Vorgehensweise

1. Montieren Sie den PRA-ES8P2S Ethernet-Switch im PRAESENSA-Baugruppenrahmen. Installieren Sie PRA-SCL und AVENAR panel bündig in einem Raum. Montieren Sie den PRA-ES8P2S Ethernet-Switch nicht im AVENAR panel Gehäuse.
2. PRAESENSA muss den Strom liefern für PRA-ES8P2S.
3. Konfigurieren Sie den PRA-ES8P2S Ethernet-Switch:
   – Erlauben Sie nur Unicast-Kommunikation zwischen FPE-8000-PPC und PRAESENSA.
   – Blockieren Sie Multicast-Kommunikation.
   – Deaktivieren Sie RSTP.
4. Überprüfen Sie den Modus von PRAESENSA, es muss im Moduls DHCP laufen. Der Modus Zeroconf wird bei der Verwendung von Smart Safety Link nicht unterstützt.
5. Verbinden Sie die PRAESENSA Steuerung über ein einzelnes Ethernet-Kabel (RSTP deaktiviert).
6. Für die Smart Safety Link Konfiguration von AVENAR panel wählen Sie **Encrypted VAS over IP** (Verschlüsseltes VAS over IP) in FSP-5000-RPS.

10.2 Mehrere direkte VAS-Schnittstellen

In einem CAN-Netzwerk kann jede Brandmelderzentrale mit einem Sprachalarmierungssystem verbunden werden. Wenden Sie die direkte Schnittstellenverbindung an, wie sie in *Eine direkte VAS-Schnittstelle, Seite 46* angegeben ist.

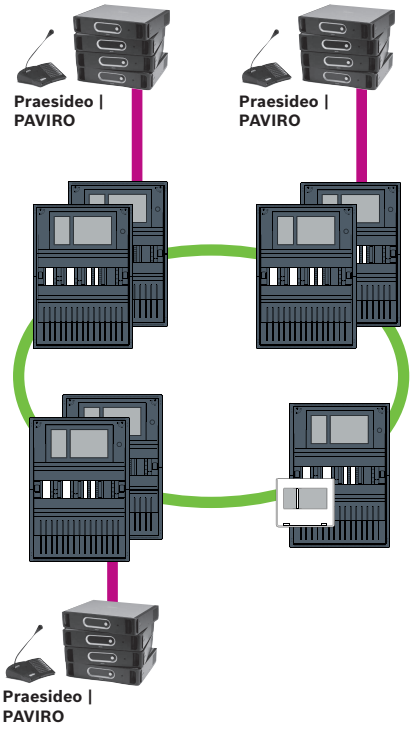


Abbildung 10.3: Mehrere direkte VAS-Schnittstellen

Führen Sie für jeden Knoten, für den Sie die Zentralen-Vernetzung über IP deaktivieren möchten, die folgenden Schritte in FSP-5000-RPS aus:

1. Wählen Sie den Knoten für die Deaktivierung der Zentralenvernetzung.
2. Wählen Sie **Ethernet-Einstellungen verwenden** aus.
3. Wählen Sie **Zentralenvernetzung über IP** nicht mehr aus.
4. Klicken Sie auf **Übernehmen**.

10.3 VAS integriert in Ethernet-Zentralennetzwerk

Wenn Praesideo und PAVIRO in Zentralennetzwerke integriert sind, dann verfügt das Sprachalarmierungssystem über einen redundanten Übertragungsweg. Der redundante Übertragungsweg ermöglicht, dass die Brandmelderzentrale und das Sprachalarmierungssystem in getrennten Räumen installiert werden.
Zurzeit ist es nicht möglich, PRAESENSA in ein Ethernet-Zentralennetzwerk zu integrieren.

Hinweis!
VdS 2540
Das Sprachalarmierungssystem muss bündig mit der Brandmelderzentrale in einem Raum untergebracht sein. Andernfalls sind die Anforderungen von VdS 2540 für Datenübertragungswege nicht erfüllt.

Hinweis!
VdS 2540 – Ethernet-Netzwerk
Bei Ethernet-Zentralennetzwerken ist zu beachten, dass für Installationen in Deutschland, wo die Einhaltung der VdS 2540 gefordert wird, Lichtwellenleiter für alle Datenübertragungswege verwendet werden müssen. Die einzige Ausnahme ist das Innere eines Gehäuses.

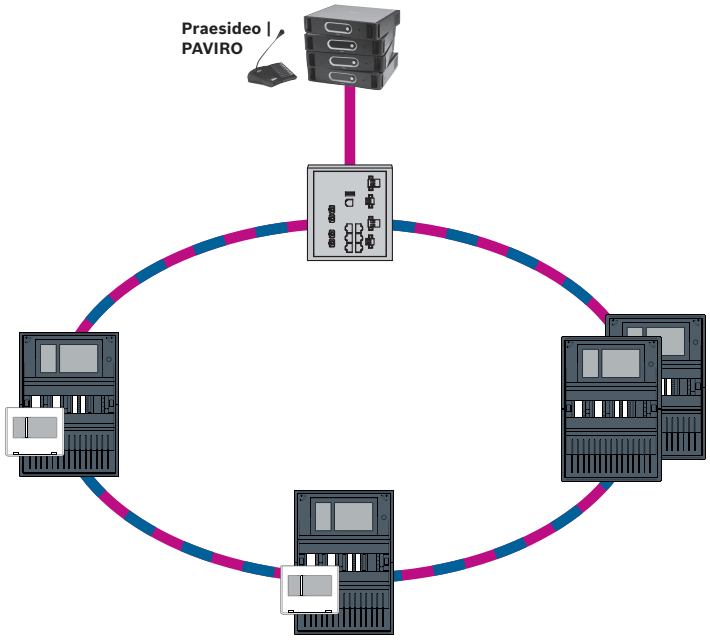


Abbildung 10.4: VAS integriert in Ethernet-Zentralennetzwerk

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. Lesen Sie den entsprechenden Abschnitt im Kapitel Installation des Handbuch Vernetzung.
Das Brandmeldesystem muss die Stromversorgung für den Ethernet-Switch sicherstellen.

11 Übergeordnete Zentrale

Ein UGM server muss in der Programmiersoftware FSP-5000-RPS erstellt werden, um eine Verbindung zu einer übergeordneten Zentrale herzustellen.
Sie müssen die folgenden Einstellungen sowohl in der Software FSP-5000-RPS als auch auf der übergeordneten Zentrale vornehmen: Programmieren Sie die logische Knotenadresse (**Netzwerkgruppe** und **Netzwerkknoten-ID**), die physikalische Knotenadresse (**PNA/RSN**) und die IP-Einstellungen (**IP-Adresse** und **Port**).
Bosch empfiehlt, den Port 25001 für die Ethernet-Schnittstelle zwischen BMZ und übergeordneter Zentrale zu verwenden.
Sie müssen jeder Zentrale oder abgesetzten Bedieneinheit einen Server zuweisen, von dem Status übertragen werden sollen. Die Anzahl der Server, die einer Zentrale oder abgesetzten Bedieneinheit zugewiesen werden können, ist begrenzt auf:

- 1 BACnet server
- 2 FSI server
- 1 OPC server
- 2 UGM server

Hinweis!
Alle Zentralensteuerungen und Server für die übergeordnete Zentrale 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.

Um eine Zentrale mit der übergeordneten Zentrale zu verbinden, müssen Sie die physische Struktur des Netzwerks in FSP-5000-RPS simulieren. Dazu gehören auch die Liniennummern zwischen der verbindenden Zentralensteuerung und den Switches der übergeordneten Zentrale.

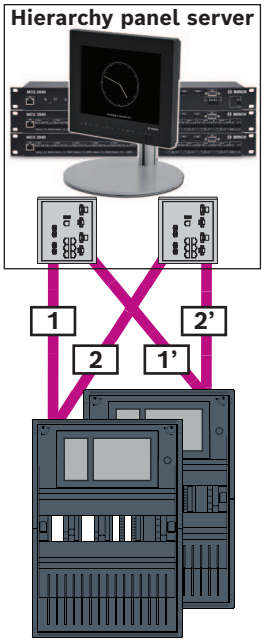


Abbildung 11.1: Beispiel für eine Liniennummerierung für die übergeordnete Zentrale

12 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.

12.1 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 Batteriereglermodul 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.

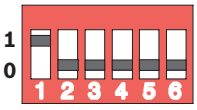
Hinweis!
Verwenden Sie für die Vernetzung nur folgende Kabel:
Ethernet-Kabel
Ethernet-Patchkabel, geschirmt, CAT5e oder besser.
Beachten Sie die in der Kabelspezifikation angegebenen minimalen Biegeradien.
Lichtwellenleiter
Multimode: Lichtwellenleiter-Ethernet-Patchkabel, Duplex I-VH2G 50/125µ oder 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-Schalternummer	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

12.2 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. Laserdiode der 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).

12.3 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 53*,
- *Redundanzeinstellungen programmieren, Seite 54*.

Weitere optionale Einstellungen, z. B.:
- *Fehlerrelais programmieren, Seite 55*,
- *Verbindungsüberwachung programmieren, Seite 55*,
- *IGMP Snooping aktivieren, Seite 56*.

12.3.1 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.

12.3.2 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** (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.

12.3.3 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 2 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 **Gerätestatus** (Device Status).
Stellen Sie unter **Diagnose (Diagnosis) -> Gerätestatus (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 **Gerätestatus** (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.

12.3.4 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** (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.

12.3.5 QoS-Priorität

Wenn Sie die Switches für die Kommunikation zwischen den Netzwerken einer BMZ und der übergeordneten Zentrale verwenden, muss die QoS-Priorität in den Switches der übergeordneten Zentrale eingestellt werden.
Ändern Sie für die übergeordneten Zentrale UGM-2040 im Menü QoS/Priorität -> Global die Einstellungen des Dropdown-Listenfeldes unter Trusted Mode auf trustIpDscp.
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.

12.3.6 IGMP Snooping aktivieren

Um das Senden von EN 54-2-relevanten Multicast-Verkehr an andere Systeme zu vermeiden, die mit dem Ethernet Switch (Sprachalarmierungssystem im Ethernet-Zentralennetzwerk integriert, 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 Querier**an.
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 unbekannten 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.

12.4 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.

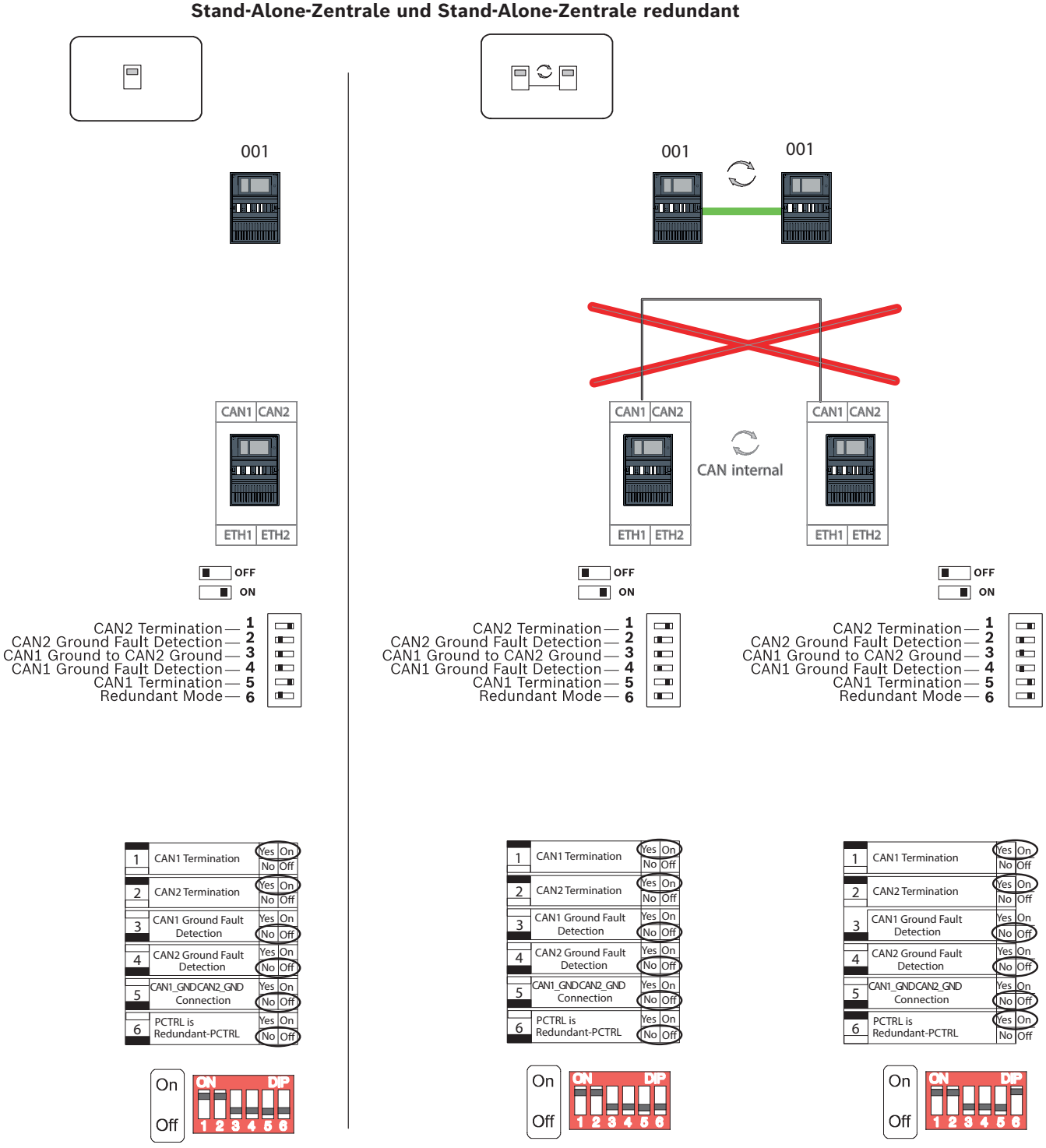


Abbildung 12.1: DIP-Schaltereinstellungen für Stand-Alone-Zentrale (oben: AVENAR, unten: FPA, links: regulär, rechts: redundant)

Abgesetzte Bedieneinheit als redundante Zentrale

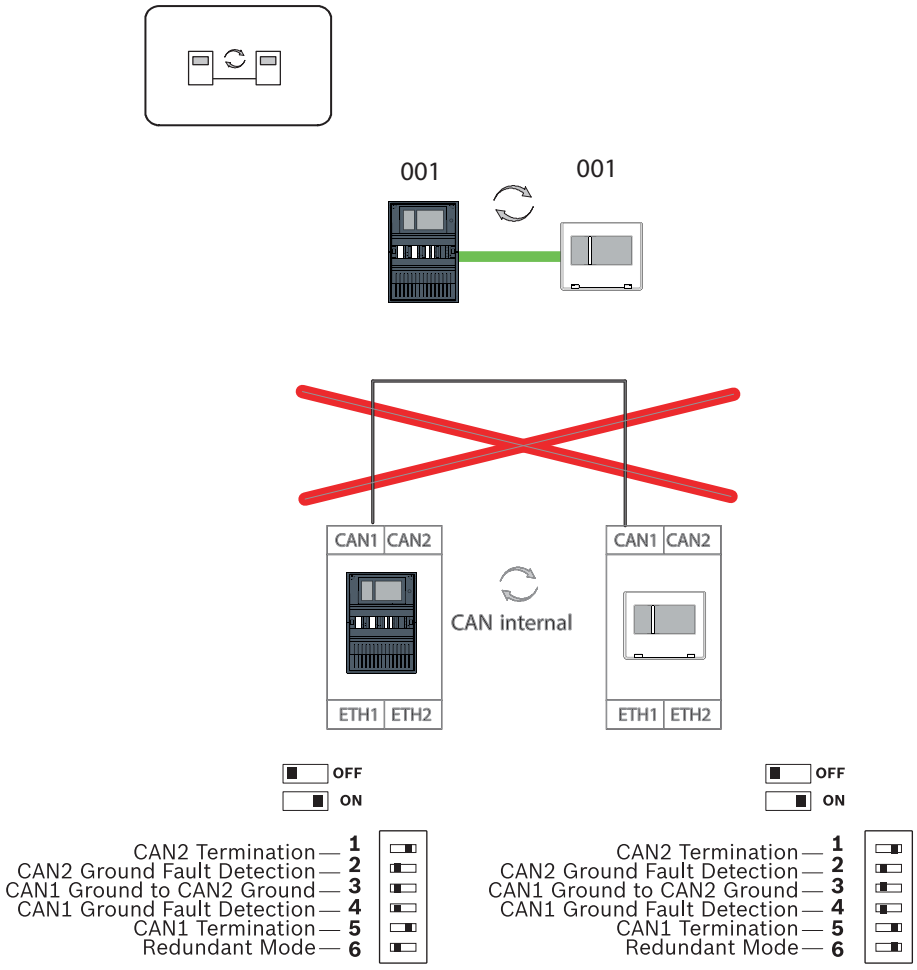


Abbildung 12.2: DIP-Schaltereinstellungen für abgesetzte Bedieneinheit als redundante Zentrale (nur AVENAR)

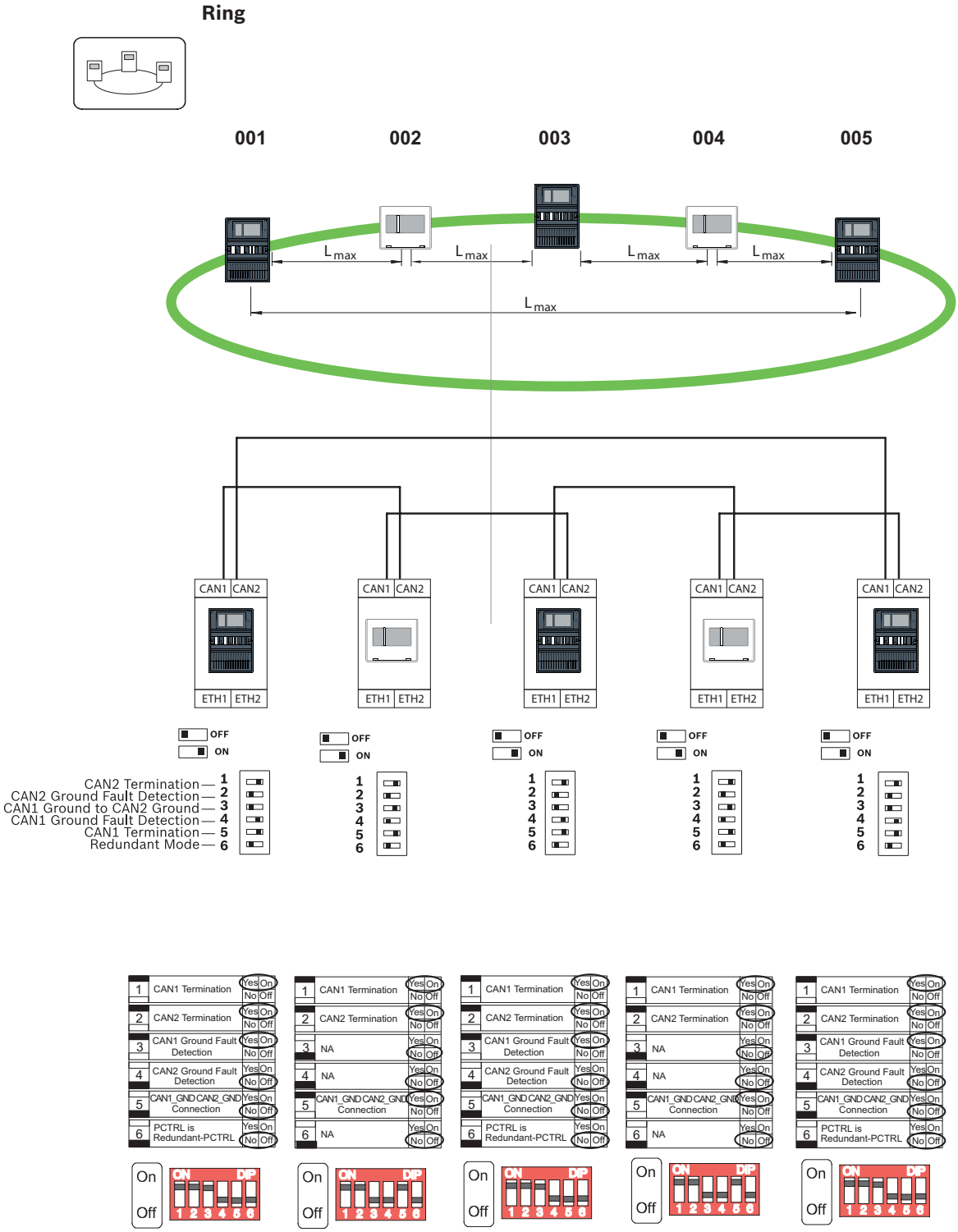


Abbildung 12.3: DIP-Schaltereinstellungen für Ring (oben: AVENAR, unten: FPA)

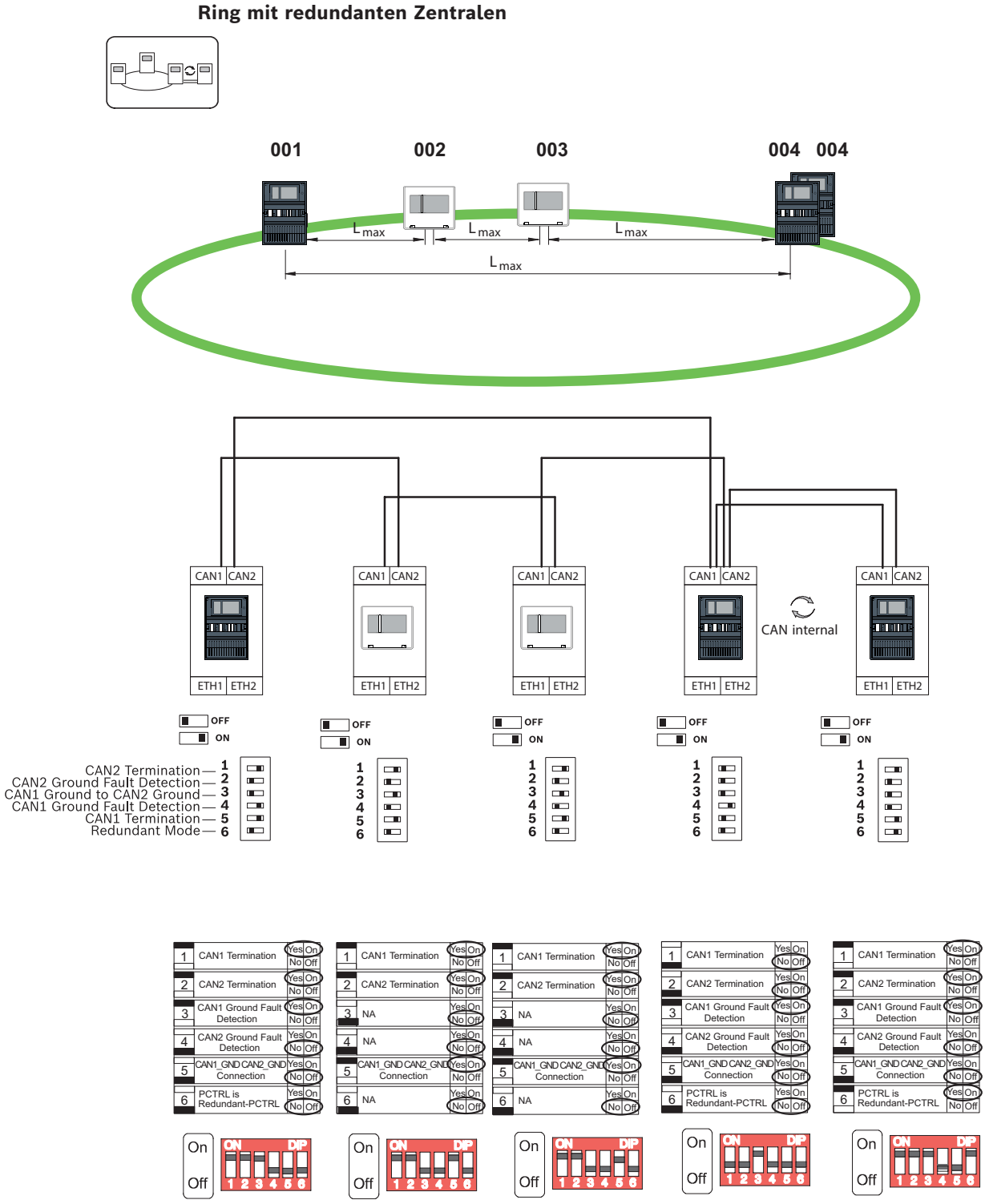


Abbildung 12.4: DIP-Schaltereinstellungen für Ring mit redundanten Zentralen (oben: AVENAR, unten: FPA)

Ring mit abgesetzter Bedieneinheit als redundante Zentrale

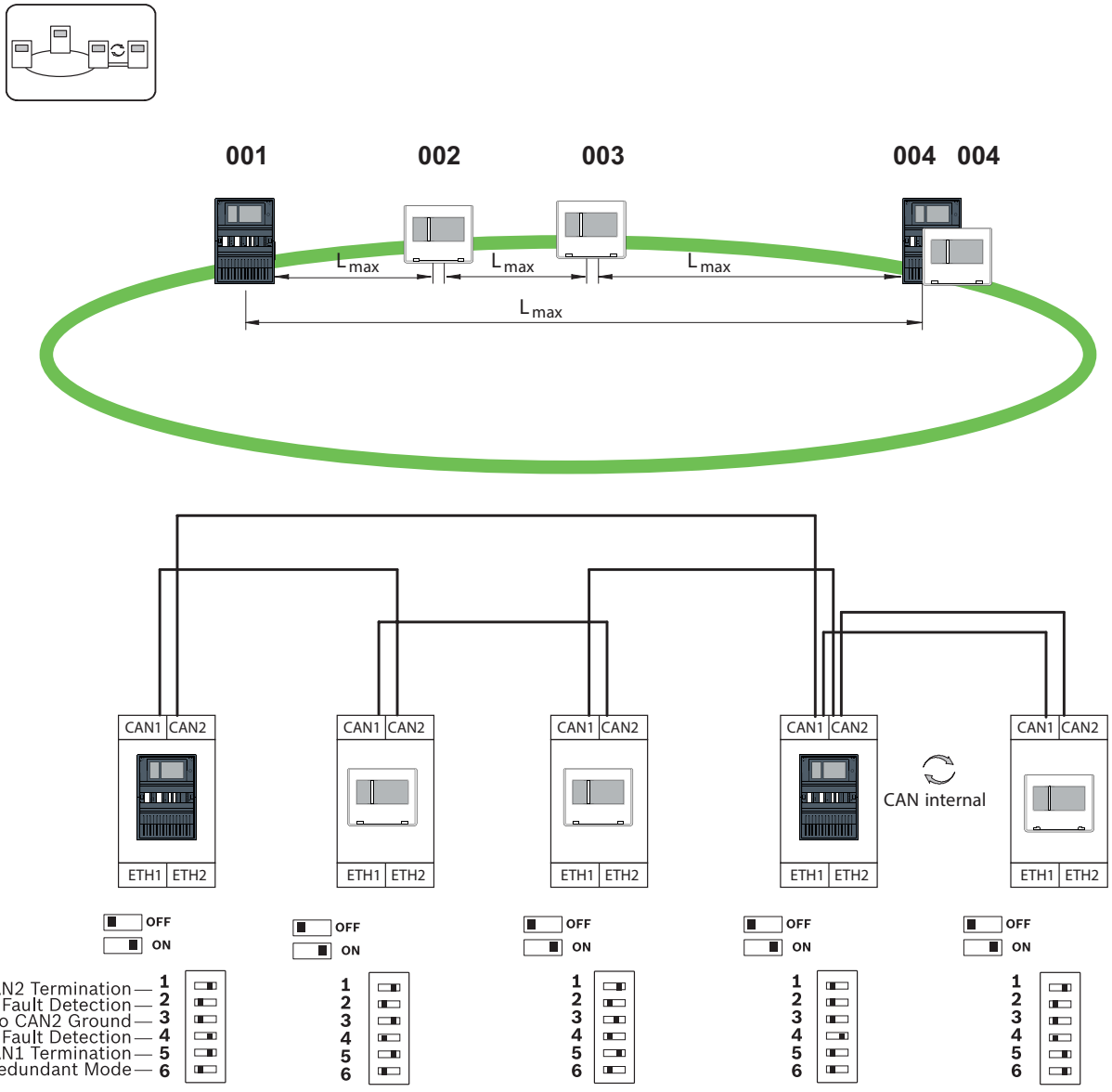


Abbildung 12.5: DIP-Schaltereinstellungen für Ring mit abgesetzter Bedieneinheit (nur AVENAR)

13 Ethernet-Verkabelung

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

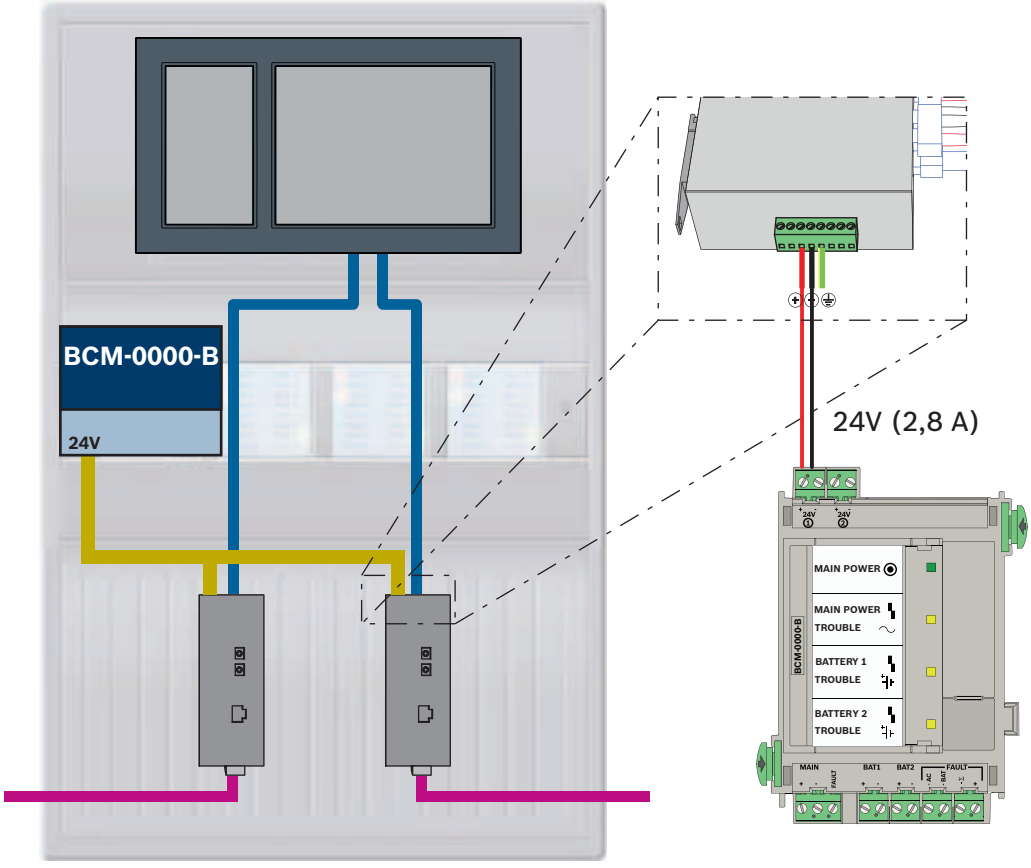
- Verwenden Sie für die Stromversorgung der Medienkonverter und der RSTP-Switches den 24-V-Ausgang des Batteriereglermoduls oder des FPP-5000 Externes Netzteil.
- Wenn Sie eine redundante Stromversorgung verbunden haben oder eine Verbindung von Switch zu Switch erstellen, müssen die Störungsausgänge 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 Medienkonverters.

Hinweis!
Verwenden Sie für die Ethernet-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, SC-Stecker.
Beachten Sie die in der Kabelspezifikation angegebenen minimalen Biegeradien.

13.1 Medienkonverter

Anschluss von Medienkonvertern

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



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

Symbol	Beschreibung
	Störungsübertragung
	Medienkonverter

13.2 Ethernet-Switch

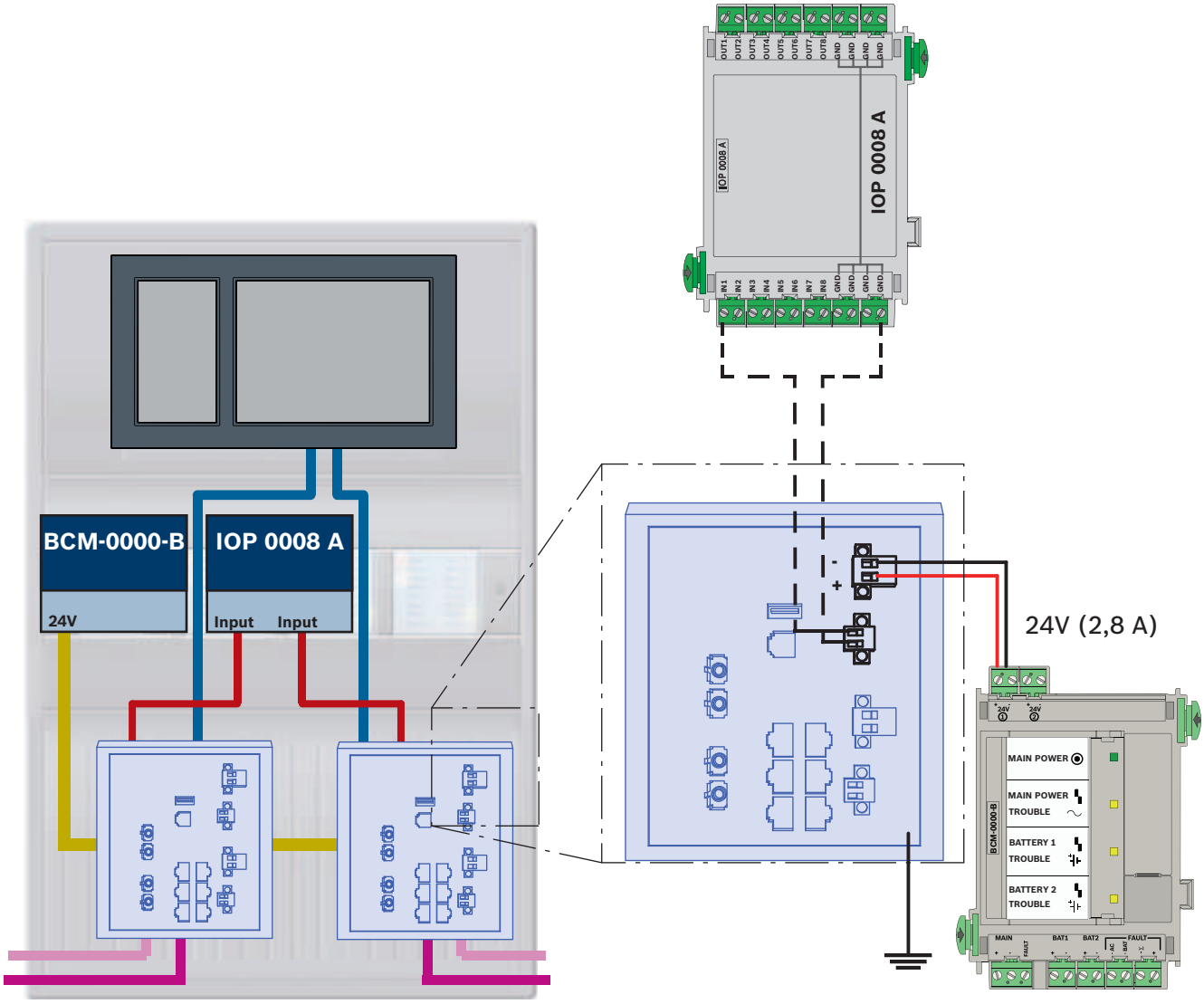
Anschaltung des Switches

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

Hinweis!

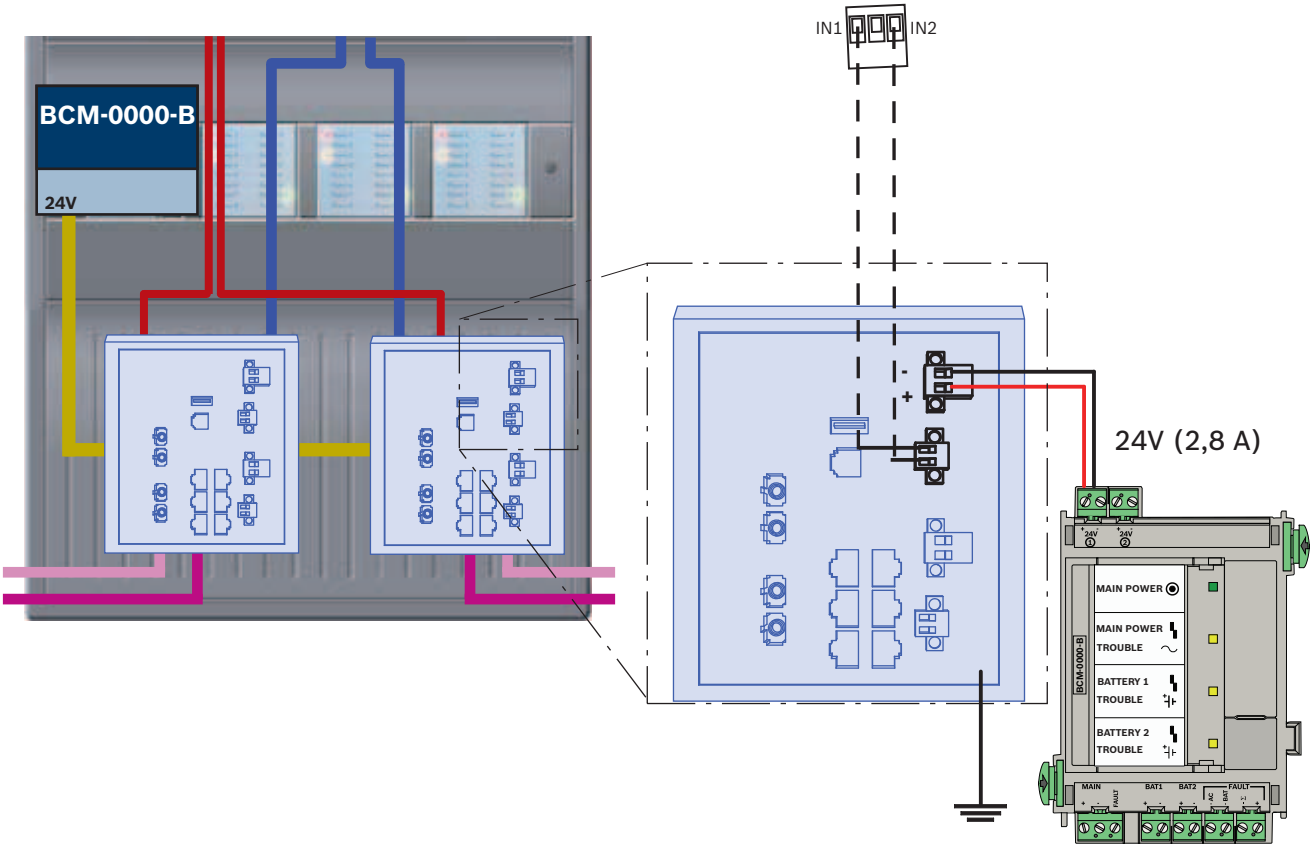
Das Störungsrelais muss nur bei Anwendungen verbunden werden, bei denen mindestens eine der folgenden Voraussetzungen erfüllt ist:
Es besteht eine Verbindung zwischen 2 Switches. Dieses ist zum Beispiel bei einem Backbone mit Sub-Ringen möglich.
Die Stromversorgung des Switches wird redundant ausgeführt.

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



Symbol	Beschreibung
	Ethernet-Kabel TX (Kupfer)
	Ethernet-Kabel FX (Lichtwellenleiter)
	Netzteil
	Störungsübertragung
	RSTP-Switch

Anschaltung von Switches mit Störungsmeldungen an die Eingänge der Zentralensteuerung



Symbol	Beschreibung
	Ethernet-Kabel TX (Kupfer)
	Ethernet-Kabel FX (Lichtwellenleiter)
	Netzteil
	Störungsübertragung
	RSTP-Switch

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

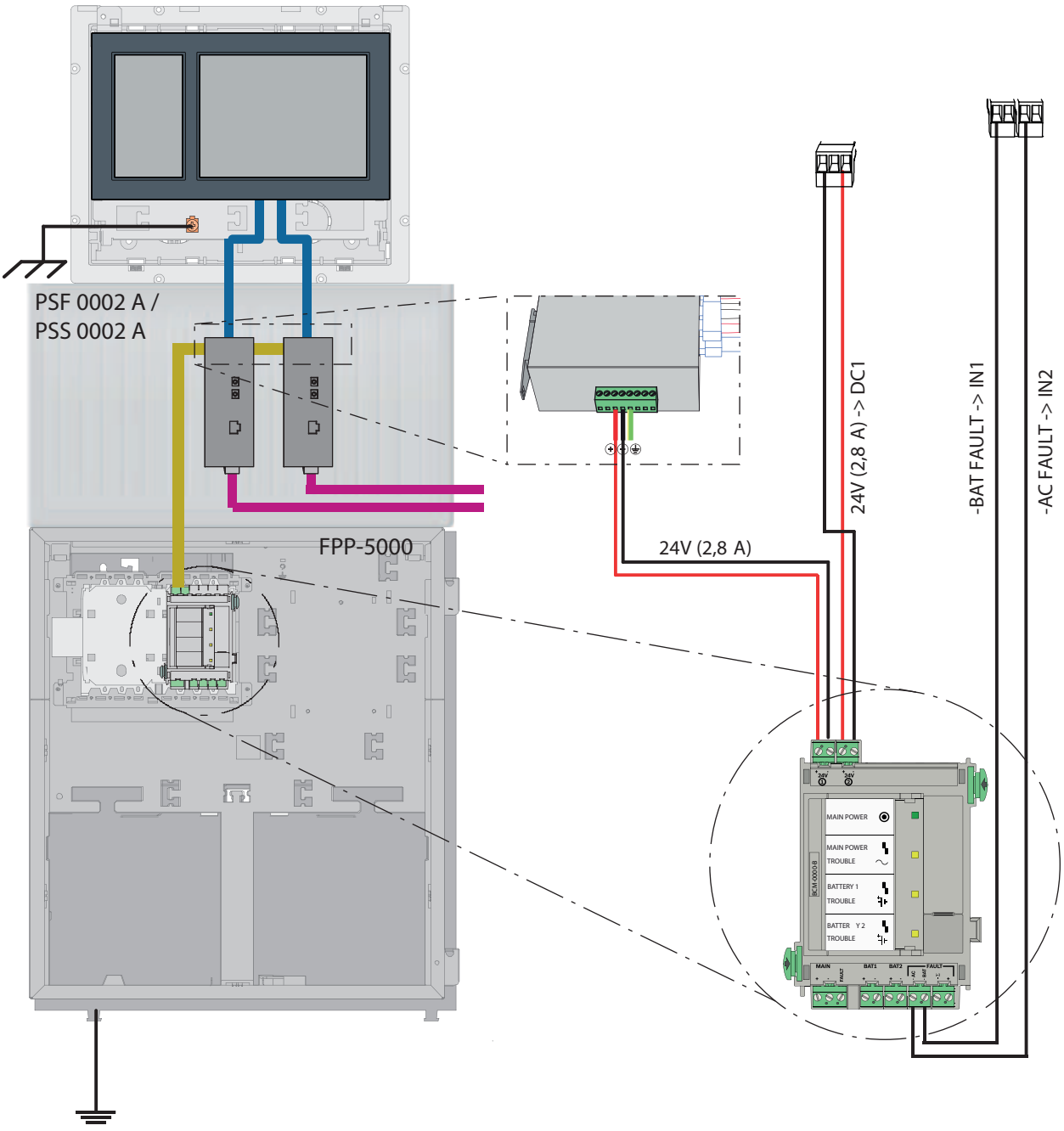
13.3 Abgesetzte Bedieneinheit

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

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.

Anschluss an abgesetzte Bedieneinheit (VdS 2540-konform)
Im Folgenden wird das externe Netzteil FPP-5000 für die Stromversorgung der abgesetzten Bedieneinheit verwendet. Die Verbindung mit dem Netzwerk wird über 2 Medienkonverter in einem PSS 0002 A oder USF 0000 A hergestellt.

Hinweis!
Das externe Netzteil FPP-5000 und ein zusätzliches Gehäuse für Medienkonverter müssen bündig mit der abgesetzten Bedieneinheit montiert werden. Die Stromversorgungskabel der abgesetzten Bedieneinheit und des Medienkonverters werden nicht auf schleichenden Kurzschluss und schleichende Unterbrechung überwacht und müssen daher in Gehäusen eingebaut werden, die bündig mit dem Gehäuse der abgesetzten Bedieneinheit montiert sind.



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

14 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.

14.1 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.
  - Legen Sie die physikalische Knotenadresse (**PNA/RSN**) an den einzelnen Knoten fest
- 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 das Gebäudemanagementsystem, das Sprachalarmierungssystem, die übergeordnete Zentrale und die 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.

14.2 Liniennummern

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.

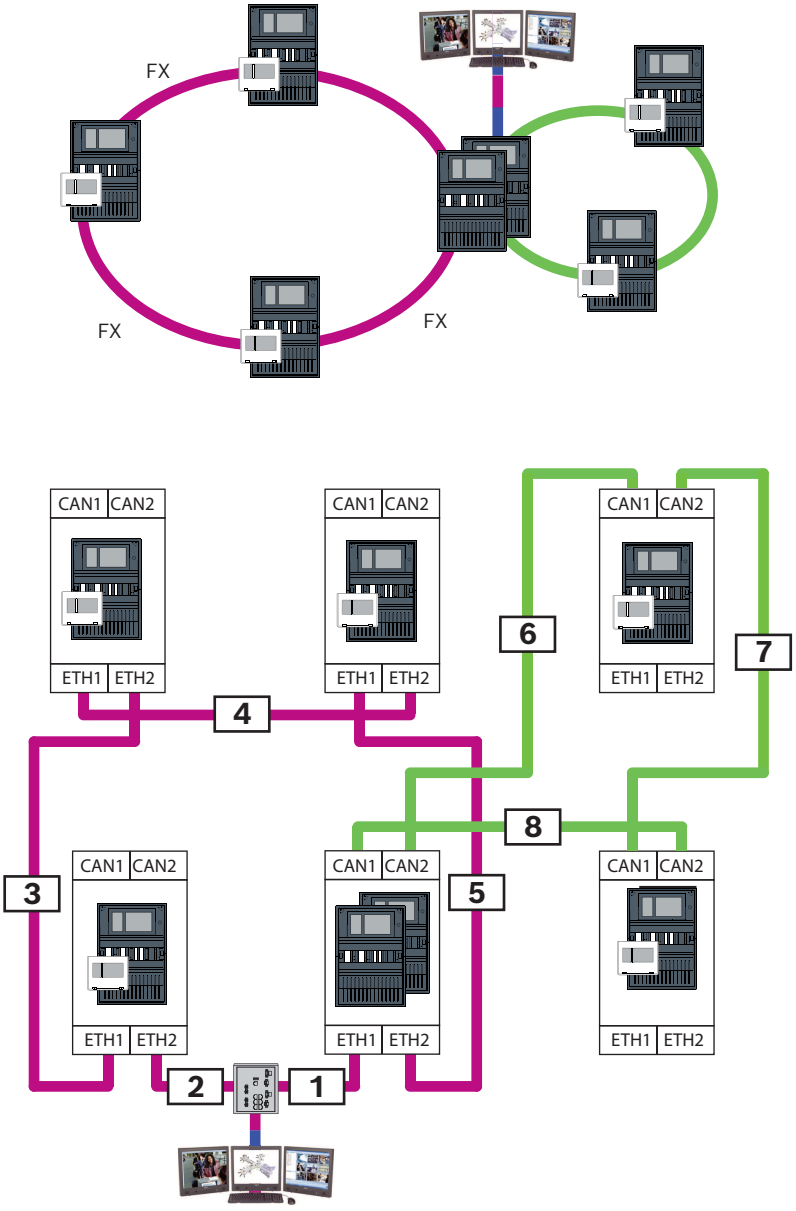


Abbildung 14.1: Beispiel eines Netzwerks und mögliche Leitungsnummerierung

14.3 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.

15 Anhang

15.1 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	**Allgemeine Netzwerkstörung**	Die Version der Zentralennetzwerksoftware ist nicht kompatibel. Es sind 2 verschiedene Softwareversionen vorhanden.
Gruppenstörungen, die sich auf das Netzwerk beziehen			
135.0.6.1	Netzwerk 2.1	**Doppelte IP-Adresse**	Eine IP-Adresse wurde zweimal vergeben.
135.0.6.2	Netzwerk 2.2	**IP-Einstellungen**	Die IP-Konfiguration der meldenden Zentrale unterscheidet sich von der RPS-Konfiguration.
135.0.6.3	Netzwerk 2.3	**Redundanzeinstellungen**	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	**RSTP-Fallback**	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	**RSTP-Topologieänderung**	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.
135.0.7.3	Netzwerk 3.3	**RSTP Link Type Point2Point**	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	**CAN 1 Störung**	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	**CAN 2 Störung**	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	**Ethernet 1 Störung**	Die Datenübertragung an Ethernet-Leitung 1 ist eingeschränkt. Mögliche Ursachen sind zum Beispiel: Kabelbrüche, Kabel nicht eingesteckt, Störeinflüsse auf das Kabel.

Physikalische Adresse	Logische Adresse	Fehlermeldung	Beschreibung und mögliche Ursache
135.0.5.4	Netzwerkverbindung 4.0	**Ethernet 2 Störung**	Die Datenübertragung an Ethernet-Leitung 2 ist eingeschränkt. Mögliche Ursachen sind zum Beispiel: Kabelbrüche, Kabel nicht eingesteckt, Störeinflüsse auf das Kabel.

Index

A

Adressvergabe
- Physikalische Knotenadresse 14

B

Building Management System 57

C

CAN-Netzwerk 9
CAN-Schnittstelle 57
CAN-Topologien 12

D

Dienste 9

E

Ethernet, Standardeinstellungen 15
Ethernet-Netzwerk 9
Ethernet-Schnittstelle 57
Ethernet-Topologien 12

G

Gebäudemanagementsystem 9, 42
Gebäudemanagementsystem, Topologien 44, 45
Grenzwerte
- Netzwerk 13

L

LLDP 20

M

MAC-Adresse 19
Maximale Grenzwerte 13

N

Netzwerk
- Adressierung 60
- Grenzwerte 13
- Kabel 25, 26
- Zentralensteuerung 57

Netzwerk: Verkabelung 25, 26
Netzwerkdurchmesser 20

P

Parameter
- RSTP 15

PAVIRO 9, 46
Physikalische Knotenadresse 14
Praesideo 9, 46

R

Redundanz
- Adressierung 14

Remote Alert 40
Remote Connect 36
Remote Maintenance 40, 41
- für privates Sicherheitsnetzwerk 41

Remote Services 36
- FSE-Mandant aktivieren 40
- Mandant erstellen 39
- Mit FSP-5000-RPS verbinden 40
- Sicheres Netzwerk-Gateway verbinden 37
- Sub-Netzwerke trennen 38

RS232-Schnittstelle 57
RSTP 20
RSTP-Parameter 15

S

Sicheres Netzwerk-Gateway 36, 37
Sprachalarmierungssystem 46
Standardeinstellungen, Ethernet 15

T

Topologien 44, 45
Topologien, CAN 12
Topologien, Ethernet 12
Topologien, mit Gebäudemanagementsystem 44, 45

U

USB-Schnittstelle 57

V

Vernetzung
- Kabellänge 25
- Ringtopologie 25

Vernetzung über CAN 9
Vernetzung über TCP/IP 9

Z

Zentralensteuerung
- Vernetzung 57

Bosch Sicherheitssysteme GmbH
Robert-Bosch-Platz 1
70839 Gerlingen
Deutschland
www.boschsecurity.com

Gebäudelösungen für ein besseres Leben

202503251706