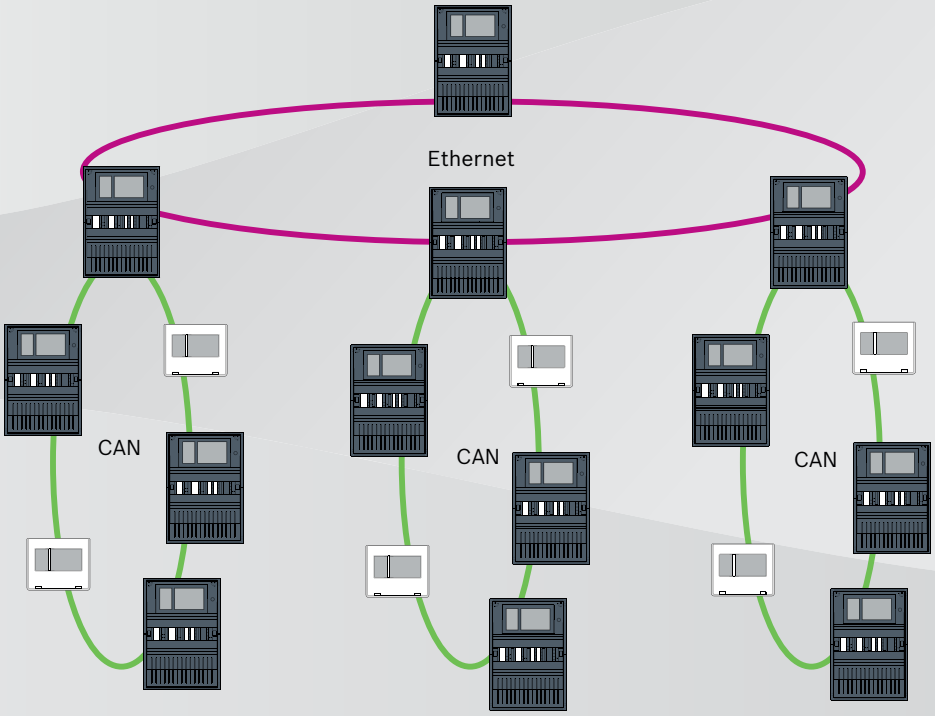
AVENAR panel Serie | FPA-5000 | FPA-1200



pl Networking manual

Spis treści

1 Bezpieczeństwo

W tym rozdziale opisano środki organizacyjne dotyczące uruchamiania klientów usługi związanych z produktami firmy Bosch na komputerze PC. Należy przestrzegać warunków tej umowy.
Podano również uwagi dotyczące bezpieczeństwa zebrane i posortowanie według tematów. W dalszej części te uwagi zostaną umieszczone przed odpowiednimi instrukcjami.

1.1 Środki organizacyjne na komputerze PC dotyczące uruchamiania klientów usługi

Wstęp

Asortyment produktów firmy Bosch związanych z zastosowaniami pożarowymi obejmuje uruchamiane na komputerze PC programy (typu usługa-klient) wymagające połączenia z systemem sygnalizacji pożaru. Ze względu na kwestie bezpieczeństwa i przepisy nie wolno instalować systemu sygnalizacji pożaru we współdzielonej sieci. Z kolei oznacza, że sieć systemu sygnalizacji pożaru i komputer, na którym uruchomiono program klienta usługi musi być fizycznie siecią dedykowaną. Ponieważ firma Bosch dostarcza tylko oprogramowanie bez stacji roboczych na których jest ono instalowane, wsparcie tych stacji jest ograniczone. Aby zmniejszyć ryzyko potencjalnych problemów związanych z bezpieczeństwem, ten dokument określa środki organizacyjne.

Środki

Jeśli środki opisane poniżej wymagają połączenia z Internetem — lub klient usługi wymaga tymczasowego połączenia z Internetem w celu uzyskania licencji — komputer musi być fizycznie odizolowany od sieci systemu sygnalizacji pożarowej przed podłączeniem go do Internetu. Przed ponownym podłączeniem komputera do sieci systemu sygnalizacji pożarowej połączenie z Internetem należy odłączyć.

1. Systemy operacyjne
   Warunki wstępne dla klientów usług określone przez firmę Bosch obejmują wersję systemów operacyjnych. Oprogramowanie klienckie jest zgodne z tymi wersjami. System operacyjny, na którym jest uruchamiany klient, musi być regularnie aktualizowany, aby zapobiec lukom w zabezpieczeniach.
   System należy skonfigurować tak, aby dostęp do zapisu był możliwy tylko dla tych folderów, które są wymagane do wykonywania danego zadania. Domyślne wszyscy użytkownicy powinni mieć uprawnienia tylko do odczytu.
2. Programy antywirusowe
   Na komputerze należy zainstalować i uruchomić najnowszy program antywirusowy. Pliki definicji wirusów muszą być regularnie aktualizowane.
3. Zapora
   Na komputerze należy zainstalować i uruchomić zaporę. Musi być ona tak skonfigurowana, aby umożliwiać ruch pomiędzy klientem usługi a systemem sygnalizacji pożaru, aktualizacje systemu operacyjnego i oprogramowania antywirusowego. Poza tym musi blokować wszelki inny ruch.
4. Bezpieczne logowanie
   Dostęp do komputera musi być ograniczony do operatorów przy użyciu klienta zainstalowanej usługi. Logowanie musi być zabezpieczone przy użyciu nowoczesnych środków W przypadku wyboru hasła jako zabezpieczenia zasady powinny wymuszać wybór hasła spełniającego aktualne reguły.
   Jeśli wymagane jest wzmocnienie uwierzytelniania, zaleca się stosowanie reguły „dwóch osób” lub uwierzytelniania wieloczynnikowego.

5. Oprogramowanie i usługi
   Liczbę programów zainstalowanych na komputerze należy ograniczyć do minimum. Należy zainstalować tylko oprogramowanie wymagane przez klienta usługi i odpowiednie zadania.
6. Ograniczenia korzystania
   Korzystanie z komputera musi być przez podjęcie odpowiednich środków organizacyjnych ograniczone do zadań związanych z usługą. Dotyczy to także korzystania z Internetu do celów innych niż opisane w niniejszym dokumencie.
7. Podział obowiązków
   Obowiązki i zakres odpowiedzialności należy odpowiednio rozdzielić, aby zmniejszyć możliwości nieuprawnionych lub niezamierzonych zmian czy niedozwolonego użycia — różne zadania należy przypisać do różnych ról.
8. Monitorowanie
   Wszystkie próby dostępu do komputera z uruchomionym klientem usługi muszą być monitorowane, aby rozpoznać nieuprawniony dostęp do komputera i Internetu.

1.2 Objaśnienie symboli bezpieczeństwa

Ostrzeżenie!
Wskazuje na niebezpieczną sytuację, która może grozić poważnymi obrażeniami ciała lub śmiercią.

Przestroga!
Wskazuje na niebezpieczną sytuację, która może grozić niewielkimi lub średnimi obrażeniami ciała.

Uwaga!
Wskazuje sytuację, która może spowodować uszkodzenie urządzenia, zagrożenie środowiska lub utratę danych.

1.3 Ostrzeżenia dotyczące bezpieczeństwa

Konwerter transmisji

Ostrzeżenie!
Światło lasera
Nie należy patrzeć wprost na wiązkę nieuzbrojonym okiem ani przez przyrządy optyczne dowolnego rodzaju (np. przez szkło powiększające lub mikroskop). Zlekceważenie tego zalecenia jest niebezpieczne dla oczu, zwłaszcza przy odległościach mniejszych niż 100 mm. Wiązka świetlna jest obecna w terminalach optycznych i na końcach podłączonych do nich kabli światłowodowych. Dioda laserowa CLASS 2M, długość fali 650 nm, wydajność < 2 mW, zgodnie z normą IEC 60825-1.

Usługi Remote Services

Przestroga!
Aby uzyskać dostęp przez Internet, należy używać tylko BoschRemote Services.

Przestroga!
Usługi Remote Serviceswymagają bezpiecznego połączenia IP. Wymagane jest połączenie z BoschRemote Services lub Private Secure Network.
Z usługą Private Secure Network udostępniana jest sieć IP poprzez DSL z opcjonalnym bezprzewodowym dostępem z centrali (EffiLink). Remote Services do sieci Private Secure Network jest dostępna tylko w Niemczech na podstawie umowy o świadczenie usług z Bosch BT-IE.

Uwaga!
Konfiguracja ustawień sieciowych centrali sygnalizacji pożarowej wymaga osobnej sieci Ethernet.
Stosowanie systemu sygnalizacji pożaru w jakiejkolwiek innej sieci Ethernet jest możliwe na własne ryzyko użytkownika. Firma Bosch nie ponosi żadnej odpowiedzialności za skutki niewłaściwego użycia.
W przypadku użycia niewyłącznej sieci Ethernet nie można zapewnić w pełni niezawodnej transmisji alarmu i bezpieczeństwa sieci IT.

Sieć central

Uwaga!
EN 54
Aby zapewnić konfigurację sieciową zgodną z normą EN 54, należy korzystać wyłącznie z elementów zatwierdzonych do użytku w sieciach obsługujących centrale sygnalizacji pożarowej.
Zewnętrzne switche RSTP i konwertery transmisji w sieciach Ethernet należy instalować w obudowach centrali. Instalacja na zewnątrz obudowy centrali jest niezgodna z normą EN 54.

Uwaga!
Długość kabla TX
Wszystkie połączenia IP muszą być bezpośrednie lub poprzez konwertery transmisji zatwierdzone przez firmę Bosch. Długość kabla TX miedzy węzłami musi być mniejsza niż 100 m.

Uwaga!
VdS 2540
Aby spełnić wymagania dyrektywy VdS 2540, należy dla torów transmisji danych używać do połączeń Ethernet kabli światłowodowych. W przypadku połączeń w obudowie można użyć kabli Ethernet TX.

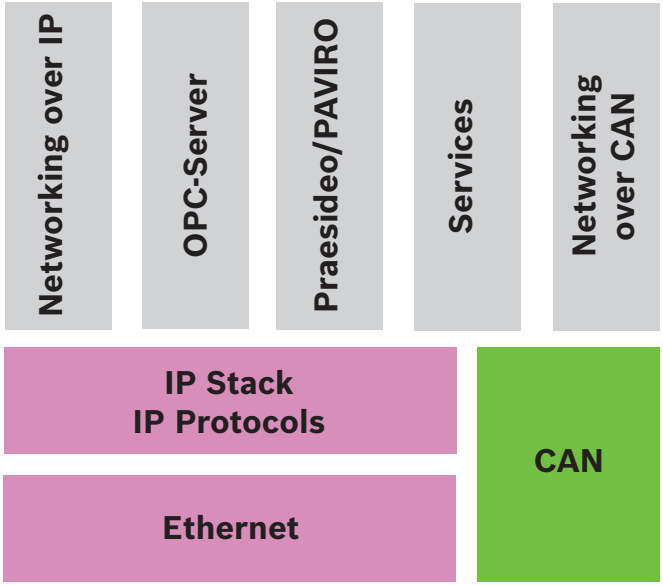
Uwaga!
W przypadku zastosowań standardowych należy używać tylko standardowych ustawień sieciowych.
Zmiany standardowych ustawień sieciowych są dozwolone tylko w przypadku doświadczonych użytkowników dysponujących odpowiednią wiedzą na temat sieci.

Uwaga!
Obowiązujące topologie
Funkcjonalność i komunikacja między centralami zależy od typu centrali. Informacje na temat usług, liczby obsługiwanych central i zdalnych klawiatur można znaleźć w specyfikacji centrali.

2 Wstęp

Niniejszy dokument jest przeznaczony dla osób mających doświadczenie w planowaniu oraz instalowaniu systemów sygnalizacji pożarowej zgodnych z normą EN 54. Dodatkowo wymagana jest wiedza na temat połączeń z siecią.
Niniejszy dokument zawiera opis różnych topologii sieci sygnalizacji pożaru. Topologie opisane są niezależnie od typu centrali sygnalizacji pożaru.
Aby utworzyć sieć centrali odpowiadającą wprowadzonej topologii i usługom łączności, wymagany jest schemat sieci opisany w tym dokumencie.
Zawiera on omówienie podstawowych warunków, wartości granicznych i ogólnych procedur dotyczących planowania oraz instalacji sieci central.
Szczegółowe opisy instalowania poszczególnych elementów można znaleźć w odpowiednich instrukcjach instalacji.
Opis interfejsu użytkownika kontrolera centrali znajduje się w podręczniku użytkownika dołączonym do urządzenia.
Interfejs użytkownika aplikacji do programowania FSP-5000-RPS został opisany w pomocy online.

3 Ogólne informacje o systemie



W sieci interfejs Ethernet i protokoły IP służą do obsługi różnych usług. Interfejs Ethernet można wyłączyć całkowicie lub tylko dla połączenia z siecią poprzezTCP/IP. Wyłączenie interfejsu może być konieczne dla połączenia poprzez CAN.

Włączanie usług

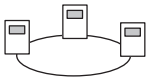
- połączenie z siecią poprzez TCP/IP
  W FSP-5000-RPS włącz komunikację między centralami w sieci Ethernet
- Serwery OPC
  Dodaj serwer OPC do konfiguracji FSP-5000-RPS.
- Połączenie z systemem Praesideo/PAVIRO
  Dodaj dźwiękowy system alarmowy do konfiguracji FSP-5000-RPS i skonfiguruj wyzwalacze wirtualne.
- Remote Services(Remote Connect jako wymóg Remote Maintenance i Remote Alert)
  Aktywuj odpowiednie pole wyboru w FSP-5000-RPS.
- Remote Services (Remote Connect jako wymóg Remote Maintenance i Remote Alert) dla sieci Private Secure Network

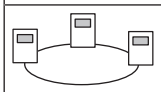
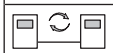
Dodaj dostęp zdalny do konfiguracji FSP-5000-RPS i skonfiguruj go w FSP-5000-RPS.

Uwaga!
Niezamierzony transfer danych
Jeśli interfejs Ethernet kontrolera centrali ma służyć jedynie do komunikacji z serwerem OPC lub usługami Remote Services wyłącz połączenie centrali z siecią poprzez TCP/IP w FSP-5000-RPS. W przeciwnym razie dane pożarowe mogą być przesyłane przez sieć Ethernet w niezamierzony sposób.

Obsługa usług opartych na sieci Ethernet lub protokole TCP/IP wymaga włączenia interfejsów Ethernet i skonfigurowania poprawnych ustawień TCP/IP.

Sieć central i zdalnych klawiatur
Poniższa tabela przedstawia opcje połączenia z siecią central/klawiatur wyniesionych w zależności od topologii sieci. Należy rozważyć ograniczenia wynikające z topologii sieci.

Topologia	**AVENAR panel 8000, licencja premium**	**AVENAR panel 8000, licencja standardowa**	**AVENAR panel 2000, licencja premium**	**AVENAR panel 2000, licencja standardowa**
 Samodzielne	Możliwe	Możliwe	Możliwe	Możliwe
 Pętla	Maks. 32 centrale/zdalne klawiatury, połączenie z urządzeniem AVENAR panel 2000, licencja premium oraz FPA	Maks. 32 centrale/zdalne klawiatury, połączenie z urządzeniem AVENAR panel 2000, licencja premium oraz FPA	Maks. 32panele/ klawiatury wyniesione, łączność z urządzeniem AVENAR panel 8000 i FPA	1 centrala i maks. 3 zdalne klawiatury
 Redundancja central	Redundantny kontroler centrali również musi być premium. Redundantną centralą może być również klawiatury wyniesiona.	Redundantny kontroler centrali może być standardowy. Redundantną centralą może być również klawiatura wyniesiona.	Niemożliwe	Niemożliwe

Topologia	**FPA-5000**	**FPA-1200**
 Samodzielne	Możliwe	Możliwe
 Pętla	Maks. 32 centrale i zdalne klawiatury	1 centrala i maks. 3 klawiatury wyniesione
	Możliwe	Brak możliwości (mikroswitch DIP 6 kontrolera centrali nie działa).

Topologia	FPA-5000	FPA-1200
Redundancja centrali		

W przypadku rozbudowania sieci FPA-5000 firma Bosch zaleca rozszerzenie jej o centralę AVENAR panel.
W przypadku wymiany centrali FPA na centralę AVENAR panel wystarczy wymienić tylko kontroler centrali. Przypomnijmy, że centrale AVENAR panel nie obsługują kart adresowych. Jeśli podłączony jest switch Ethernet, można dalej z niego korzystać.
W przypadku wymiany zdalnej klawiatury FPA na zdalną klawiaturę AVENAR panel sprawdź, czy rezystancja linii mieści się w granicach określonych dla zdalnej klawiatury AVENAR panel.

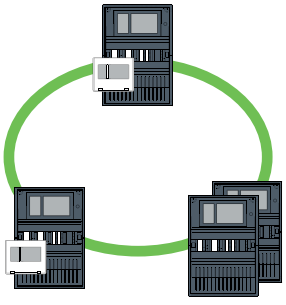
Uwaga!
Instalacja oprogramowania sprzętowego
Połączone centrale muszą mieć tę samą wersję oprogramowania sprzętowego.
Instalacja oprogramowania sprzętowego jest możliwa tylko na aktywnej centrali. W przypadku central redundantnych instalację oprogramowania sprzętowego należy wykonać na obu centralach. W tym celu należy zmienić role central i przywrócić je po pomyślnym wykonaniu instalacji oprogramowania sprzętowego.

Uwaga!
Redundantny kontroler centrali
Nie można łączyć ze sobą kontrolerów centrali AVENAR panel i FPA w celu uzyskania redundancji.

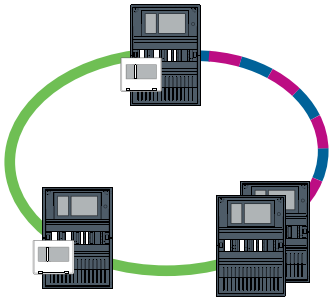
4 Topologie

Niniejszy dokument zawiera opis różnych topologii sieci sygnalizacji pożaru. Topologie opisane są niezależnie od typu centrali sygnalizacji pożaru.

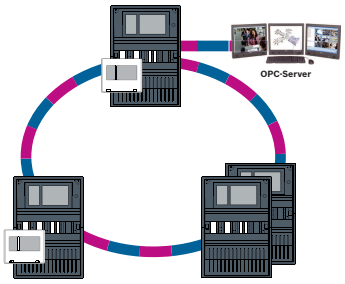
Uwaga!
Obowiązujące topologie
Funkcjonalność i komunikacja między centralami zależy od typu centrali. Informacje na temat usług, liczby obsługiwanych central i zdalnych klawiatur można znaleźć w specyfikacji centrali.



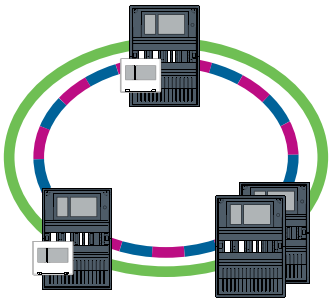
Pętla CAN, Strona 15



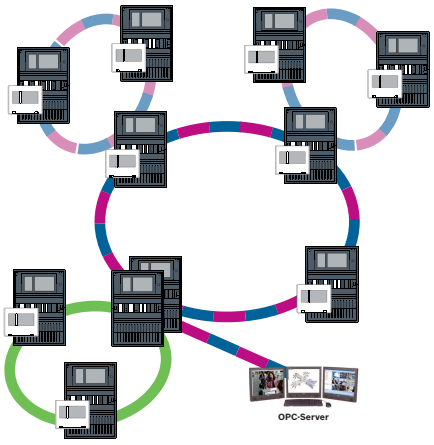
Pętla CAN z segmentami sieci Ethernet, Strona 17



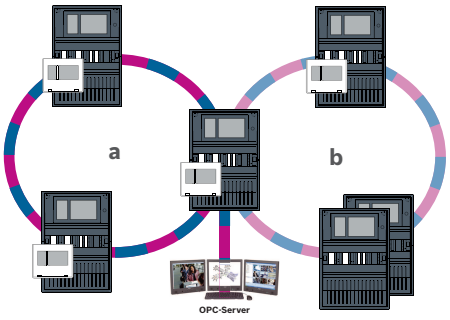
Pętla Ethernet, Strona 16
Pętla Ethernet z serwerem OPC, Strona 16
Pętla Ethernet z serwerem OPC do centrali redundantnej, Strona 17



Podwójna pętla Ethernet/CAN, Strona 17

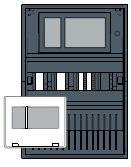
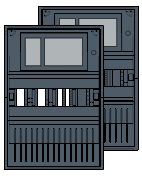


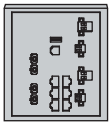
Sieć szkieletowa Ethernet z podpętlami (Ethernet/CAN), Strona 17



Podłączanie pętli Ethernet, Strona 19

Kabel	Opis
	Kabel Ethernet TX (miedziany), długość kabla TX pomiędzy węzłami < 100 m
	Kabel Ethernet FX (kabel światłowodowy)
	Kabel Ethernet TX lub FX, długość kabla TX pomiędzy węzłami < 100 m
	Kabel CAN, długość kabla CAN między węzłami < 1000 m

Urządzenie	Opis
	Centrala lub zdalna klawiatura (w topologii sieci Ethernet jeden wewnętrzny switch RSTP dla każdego elementu)
	Nadmiarowa centrala (w topologii sieci Ethernet wewnętrzny switch RSTP)

Urządzenie	Opis
	Klawiatura wyniesiona może być używana jako redundantny kontroler centrali. Połączenia sieciowe i ustawienia są identyczne dla redundantnego kontrolera centrali i redundantnej klawiatury. Używanie redundantnej klawiatury ma zastosowanie wyłącznie do AVENAR panel 8000.
	Przełącznik sieci Ethernet jako zewnętrzny switch RSTP (ogólnie switch Ethernet MM)
	Konwerter transmisji
	Bezpieczna brama sieciowa usług Remote Services

Ograniczenia w sieci

Liczba central i zdalnych klawiatur, które mogą być połączone w sieć, zależy od wybranej topologii sieci.

Połączone w sieć centrale i zdalne klawiatury nazywane są węzłami.

- Liczba punktów detekcji w sieci jest ograniczona do 32768.
- Liczba punktów detekcji na centrale działającą w sieci jest ograniczona do 2048.
- Liczba węzłów w systemie zależy od typu topologii.
  Węzłem jest albo kontroler centrali, albo zdalna klawiatura.
- Liczba węzłów w topologii pętli jest ograniczona do 32.
- Za pomocą oprogramowania FSP-5000-RPS do jednej centrali można przypisać maksymalnie 3 skonfigurowane zdalne klawiatury.

Okablowanie pomiędzy węzłami i maksymalna dopuszczalna długość kabla zależą również od wybranej topologii.

Sieć może być utworzona maksymalnie z 32 kontrolerów centrali, zdalnych klawiatur i serwerów OPC.

W zależności od konkretnego zastosowania różne kontrolery centrali i zdalne klawiatury można dzielić na grupy i definiować jako węzły sieciowe lub lokalne. Jest zasadą, że w obrębie grupy można wyświetlać wyłącznie stan central należących do danej zdefiniowanej grupy. Stan wszystkich central można wyświetlać i/lub przetwarzać z poziomu węzłów sieci niezależnie od grupy, do której należą centrale.

Adres węzła fizycznego

Centrala lub zdalna klawiatura są identyfikowane w sieci za pomocą unikatowych adresów zwanych adresami węzła fizycznego.

Uwaga!

Adres węzła fizycznego redundantnych centrali

Centrala redundantna musi mieć ustawioną ten sam adres węzła fizycznego co centrala główna.

Uwaga!

Używana sieć musi spełniać następujące wymagania minimalne:

Minimalna przepustowość: 1 Mb/s

Maksymalne opóźnienie: 250 ms

Uwaga!
EN 54
Aby zapewnić konfigurację sieciową zgodną z normą EN 54, należy korzystać wyłącznie z elementów zatwierdzonych do użytku w sieciach obsługujących centrale sygnalizacji pożarowej.
Zewnętrzne switche RSTP i konwertery transmisji w sieciach Ethernet należy instalować w obudowach centrali. Instalacja na zewnątrz obudowy centrali jest niezgodna z normą EN 54.

Uwaga!
Centrala redundantna — EN 54-2
Zgodnie z normą EN 54-2 dla każdej centrali można podłączyć maksymalnie 512 punktów detekcji. W przypadku przekroczenia tej liczby centrala musi być zaprojektowana redundantnie.
Jeśli centrala działa jako interfejs z podpętlą CAN i więcej niż 512 punktami detekcji w podpętli, to należy ją również zaprojektować redundantnie. Przełącznik RSTP, który łączy 2 pętle, zapewnia redundancję.
W przypadku centrali samodzielnej można podłączyć 4096 punktów detekcji, nawet jeśli została ona zaprojektowana jako redundantna. Jeśli centrala znajduje się w sieci, można podłączyć maksymalnie 2048 punktów detekcji.

Uwaga!
Upewnij się, że adres węzła fizycznego przypisany do centrali pasuje do adresu węzła fizycznego określonego w aplikacji do obsługi programowania. Odpowiada on za ustawienie ostatniego numeru adresu IP w ustawieniach standardowych.
Aktywuj opcję RSTP jako protokół redundancji i przyjmij domyślne wartości standardowe.

Standardowe ustawienia Ethernet centrali sygnalizacji pożaru
W standardowych ustawieniach centrali sygnalizacji pożaru aplikacja do programowania FSP-5000-RPS oraz moduł sterujący przyjmują ustawienie adresu węzła fizycznego takie jak ostatnia cyfra w adresie IP.

Uwaga!
Poprawne ustawienie adresu węzła fizycznego w kontrolerach centrali i aplikacji do programowania FSP-5000-RPS jest koniecznym warunkiem działania sieci.

Uwaga!
Użycie redundancji sieci Ethernet należy aktywować oddzielnie w kontrolerze centrali.

- Ustawienia IP
  - Adres IP 192.168.1.x
    Ostatnia cyfra adresu IP w ustawieniach standardowych jest zawsze identyczna z ustawieniem adresu węzła fizycznego w kontrolerze centrali.
  - Ekran sieciowy 255.255.255.0
  - Brama 192.168.1.254
  - Adres multiemisji 239.192.0.1
  - Numer portu 25001–25008 (można ustawić tylko pierwszy port; zawsze używanych jest 8 kolejnych portów)
- RSTP (ustawienia domyślne)

- Bridge Priority 32768
- Hello Time 2
- Max. Age 20
- Forward Delay 15

Uwaga!
Ustawienia standardowe konfiguracji IP można stosować w sieciach obejmujących maksymalnie 20 switchów RSTP.
W przypadku sieci z liczbą switchów większą niż 20 RSTP wymagane są dodatkowe ustawienia odpowiadające topologii. Potrzebna jest do tego dogłębna znajomość zagadnień sieciowych.

Ustawienia pętli obejmujących więcej niż 20 switchów RSTP

Jeśli sieć obejmuje ponad 20 switchów RSTP, konieczne jest dopasowanie ustawień RSTP w kontrolerze centrali i aplikacji do programowania. Kontrolery centrali, zdalne klawiatury i podłączone switche zewnętrzne RSTP są traktowane jako switche RSTP. Nadmiarowe kontrolery centrali nie są traktowane jak switche RSTP, ponieważ znajdujący się w nich switch nie działa jako switch RSTP.

- RSTP
  - Zachowaj Bridge Priority 32768
  - Zachowaj Hello Time 2
  - Zmień Max. Age z 20 na 40
  - Zmień Forward Delay z 15 na 25

Parametry

- W pętli można wykorzystać maksymalnie 32 węzły.
- Średnica sieci nie może być większa niż 32, patrz *Średnica sieci, Strona 22*.
- Przełączniki Ethernet nie mogą być używane na zewnątrz obudów central.
- Konwertery transmisji nie mogą być używane na zewnątrz obudów central.

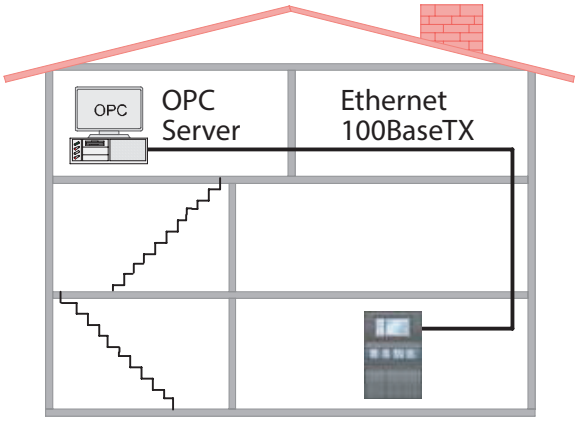
Funkcje

- Sieć jest zgodna z normą EN 54.
- Sieć korzysta z RSTP.

Podłączanie do systemu BIS z serwerem OPC

W przypadku podłączania do systemu zarządzania budynkiem (BIS) za pośrednictwem serwera OPC i Ethernet 100BaseTX w sieciach wielu budynków należy ustalić z administratorem sieci, czy:

1. Sieć jest przeznaczony dla wielu budynków? (np. nie może powodować zakłóceń technicznych ze względu na różnice potencjału uziemienia)
2. Przepustowość wykorzystywana przez użytkowników magistrali jest wystarczająca dla sieci.



Rysunek 4.1: Połączenie do systemu BIS za pośrednictwem serwera OPC

Informacje dodatkowe na temat użycia serwera OPC

Serwery OPC w sieci muszą być dodane do aplikacji programującej FSP-5000-RPS.
W oprogramowaniu FSP-5000-RPS i na serwerze OPC muszą być skonfigurowane następujące ustawienia:

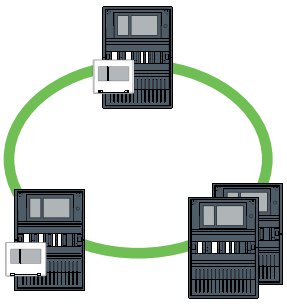
- Węzły sieci
- Grupa sieciowa
- RSN
- Adresy IP
- Port

Serwer OPC używa portu 25000 standardowo.

Uwaga!
EN 54
Połączenie systemu wizualizacji (np.BIS) za pośrednictwem interfejsu Ethernet przy użyciu serwera OPC lub serwera FSI jest zgodne z normą EN54, jeśli odpowiednie funkcje EN54 są wykonywane wyłącznie przez centralę sygnalizacji pożaru. Każda metoda kontroli lub administracji zgodna z normą EN54 (np. kontrola sygnalizatorów lub wyłączanie elementów) dostępna w systemie wizualizacji wymaga zastosowania certyfikowanego systemu integrującego.

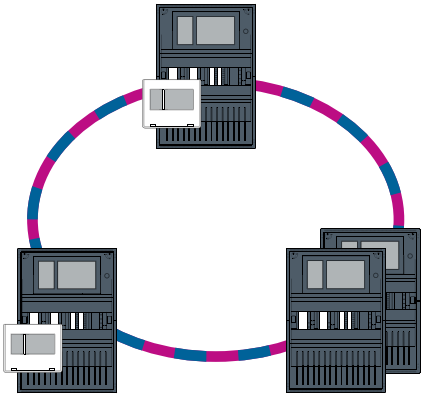
Uwaga!
Aplikacja do programowania FSP-5000-RPS
Należy pamiętać o przypisaniu serwera OPC do każdego węzła sieci, z którego mają być przesyłane informacje o stanie.

4.1 Pętla CAN



Rysunek 4.2: Pętla CAN

4.2 Pętla Ethernet



Rysunek 4.3: Pętla Ethernet

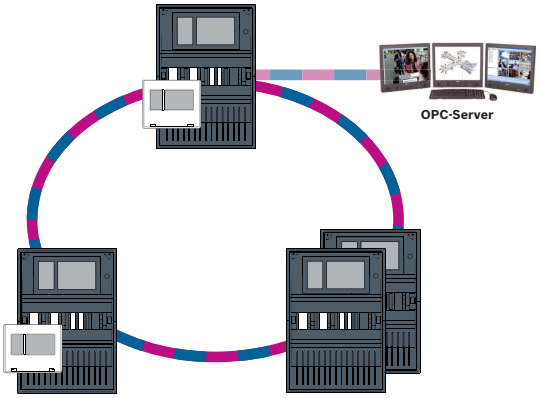
4.3 Pętla Ethernet z serwerem OPC

Przełącznik Ethernet do podłączania serwera OPC musi być zaprogramowany oddzielnie.
Aby uzyskać informacje o programowaniu ustawień adresu IP i nadmiarowości przełącznika Ethernet, patrz *Ustawienia przełącznika, Strona 45*. Ze względu na to, że przełącznik jest instalowany w bezpośrednim sąsiedztwie (bez wolnej przestrzeni), nie jest konieczne projektowanie nadmiarowego zasilania. Dlatego też wyjścia sygnału awarii nie są używane. Należy upewnić się, że ustawienia RSTP w kontrolerach central, w aplikacji do programowania FSP-5000-RPS i przełączniku Ethernet są identyczne.

Serwer OPC musi być zaprogramowany oddzielnie.
Zaprogramuj adres IP, węzły sieci, grupy sieciowe i RSN. Zobacz odpowiednią część w rozdziale dotyczącym instalacji, w instrukcji połączeń z siecią.
Standardowo serwer OPC używa portu 25000.
Należy upewnić się, że ustawienia w aplikacji do programowania FSP-5000-RPS i serwera OPC są identyczne.

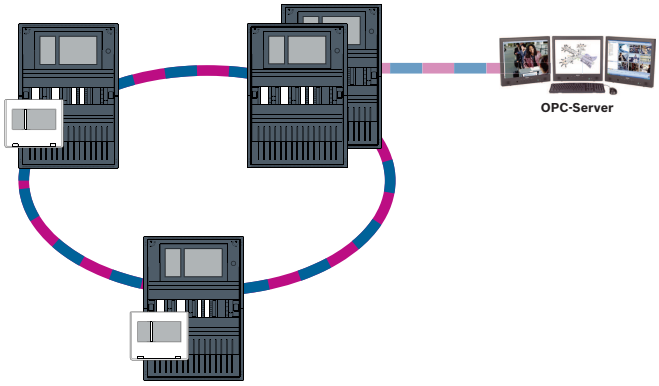
Parametry

– Serwer OPC może być podłączony za pośrednictwem kabla Ethernet (miedzianego) lub kabla światłowodowego.



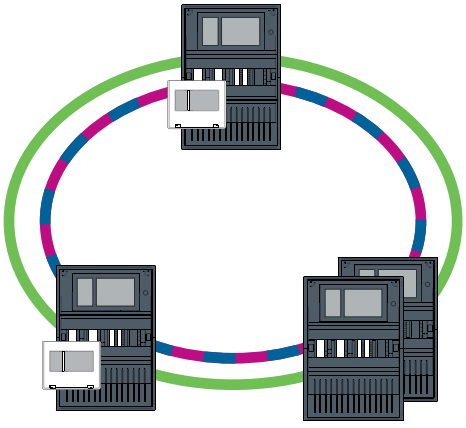
Rysunek 4.4: Pętla Ethernet z serwerem OPC

4.4 Pętla Ethernet z serwerem OPC do centrali redundantnej



Rysunek 4.5: Pętla Ethernet z serwerem OPC do centrali nadmiarowej

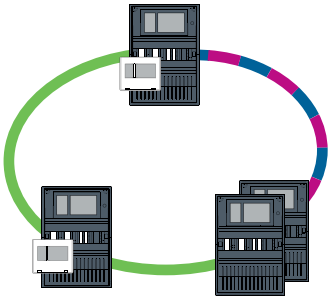
4.5 Podwójna pętla Ethernet/CAN



Rysunek 4.6: Podwójna pętla Ethernet i CAN

4.6 Pętla CAN z segmentami sieci Ethernet

Topologia główna jest pętlą CAN. Gdy odległość między dwoma węzłami jest dłuższa 1000 m, można użyć połączenia Ethernet FX.



Rysunek 4.7: Pętla CAN z segmentami sieci Ethernet

4.7 Sieć szkieletowa Ethernet z podpętlami (Ethernet/CAN)

Sieć szkieletowa Ethernet jest podłączona do wszystkich podpętli i dlatego łączy istotny obszar z dużą przepustowością. Przełączniki w sieci szkieletowej nie są domyślnie nadrzędne. Należy pamiętać, że ta topologia wymaga określenia średnicy sieci. Kontrolery centrali, zdalne klawiatury i podłączone przełączniki zewnętrzne RSTP są traktowane jako przełączniki RSTP. Połączone w sieć CAN centrale nie są uwzględniane podczas określania średnicy sieci.

Rozważając ustawienia dla pętli obejmujących więcej niż 20 przełączników RSTP, należy wziąć pod uwagę informacje podane w *Ustawienia pętli obejmujących więcej niż 20 switchów RSTP, Strona 14*.

Uwaga!
Ta topologia wymaga dodatkowej konfiguracji ustawień dla wszystkich przełączników RSTP w sieci szkieletowej. Potrzebna jest do tego dogłębna znajomość zagadnień sieciowych.

Uwaga!
W przypadku gdy centrala działa jako interfejs z podpętlą CAN, również musi być zaprojektowana nadmiarowo (zgodnie z normą EN 54-2), jeśli w podpętli podłączono więcej niż 512 punktów detekcji.
Ograniczenie to nie dotyczy pętli Ethernet, ponieważ przełączniki służące do połączenia dwóch pętli obsługują nadmiarowość.

Ustawienia dodatkowe
Pętla centralna musi działać jako sieć szkieletowa. Musi być ona połączona w sieć za pośrednictwem sieci Ethernet.

Uwaga!
Dla wszystkich przełączników RSTP w sieci szkieletowej należy ustawić priorytet RSTP wyższy niż w podpętlach. Dzięki temu most główny RSTP zawsze pozostanie w sieci szkieletowej, nawet w przypadku usterki.
Przełączniki RSTP podłączające pętle są częścią sieci szkieletowej!
W sieci szkieletowej należy używać priorytetu RSTP 16384.

Uwaga!
Im niższa jest wartość ustawienia, tym wyższy priorytet RSTP.

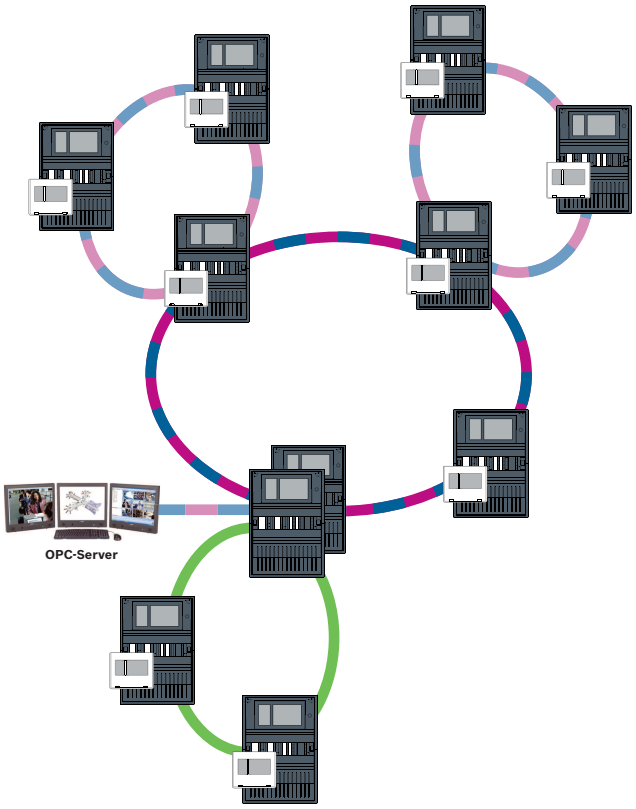
Przełączniki do podłączenia serwera OPC i podpętli muszą być zaprogramowane oddzielnie.
Aby uzyskać informacje o programowaniu ustawień adresu IP i nadmiarowości przełączników Ethernet, patrz *Ustawienia przełącznika, Strona 45*. W przypadku tej topologii użycie wyjść sygnału usterki przełącznika jest konieczne, jeśli zaprojektowano nadmiarowe zasilanie przełącznika lub istnieje połączenie typu przełącznik-przełącznik (patrz *Przełącznik Ethernet, Strona 56*).
Należy upewnić się, że ustawienia RSTP w kontrolerach central, w aplikacji do programowania FSP-5000-RPS i przełączniku Ethernet są identyczne.

Uwaga!
Zmień priorytet RSTP przełączników RSTP łączących pętle, jeśli należą do sieci szkieletowej.

Serwer OPC musi być zaprogramowany oddzielnie.
Aby uzyskać informacje o programowaniu adresu IP, węzłów sieci, grupy sieciowej i RSN, patrz *Serwery OPC, Strona 62*.
Standardowo serwer OPC używa portu 25000.
Należy upewnić się, że ustawienia w aplikacji do programowania RPS i serwera OPC są identyczne.

Parametry

– Serwer OPC może być podłączony za pośrednictwem kabla Ethernet (miedzianego) lub kabla światłowodowego.



Rysunek 4.8: Sieć szkieletowa Ethernet z podpętlami

4.8 Podłączanie pętli Ethernet

Uwaga!
Ta topologia wymaga dodatkowej konfiguracji ustawień dla wszystkich przełączników RSTP w sieci szkieletowej. Potrzebna jest do tego dogłębna znajomość zagadnień sieciowych.

Ustawienia dodatkowe
Niniejsza topologia jest szczególnym przykładem sieci szkieletowej Ethernet z podpętlami (patrz Sieć szkieletowa Ethernet z podpętlami (Ethernet/CAN)). Jedna z dwóch pętli musi działać jako sieć szkieletowa.

Uwaga!
Dla wszystkich central i przełączników w sieci szkieletowej należy ustawić priorytet RSTP wyższy niż w podpętlach. Dzięki temu most główny RSTP zawsze pozostanie w sieci szkieletowej, nawet w przypadku usterki.
Przełączniki podłączające dwie pętle są częścią sieci szkieletowej!
W sieci szkieletowej należy używać priorytetu RSTP 16384.

Uwaga!
Im niższa jest wartość ustawienia, tym wyższy priorytet RSTP.

Przełączniki do podłączenia serwera OPC i drugiej pętli muszą być zaprogramowane oddzielnie.

Aby uzyskać informacje o programowaniu ustawień adresu IP i nadmiarowości przełącznika Ethernet, patrz *Ustawienia przełącznika, Strona 45*. W przypadku tej topologii użycie wyjść sygnału usterki przełącznika jest konieczne tylko wtedy, jeśli zaprojektowano nadmiarowe zasilanie przełącznika, patrz *Przełącznik Ethernet, Strona 56*.

Należy upewnić się, że ustawienia w kontrolerach central, aplikacji do programowania FSP-5000-RPS i przełączniku Ethernet są identyczne.

Należy zmienić priorytet RSTP przełączników łączących dwie pętle, jeśli należą do sieci szkieletowej.

Serwer OPC musi być zaprogramowany oddzielnie.

Zaprogramuj adres IP, węzły sieci, grupy sieciowe i RSN. Zobacz odpowiednią część w rozdziale dotyczącym instalacji, w instrukcji połączeń z siecią.

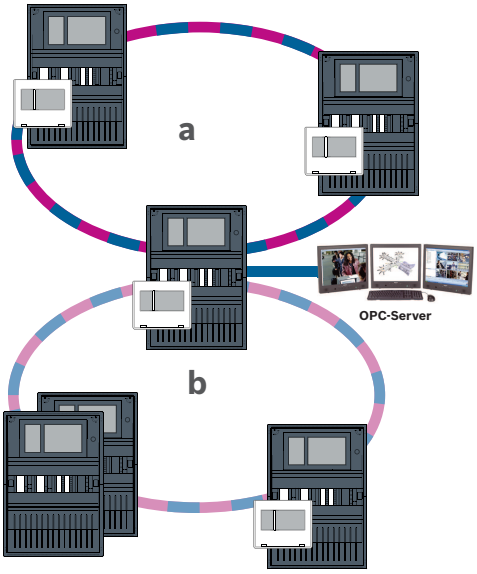
Standardowo serwer OPC używa portu 25000.

Należy upewnić się, że ustawienia w aplikacji do programowania FSP-5000-RPS i serwera OPC są identyczne.

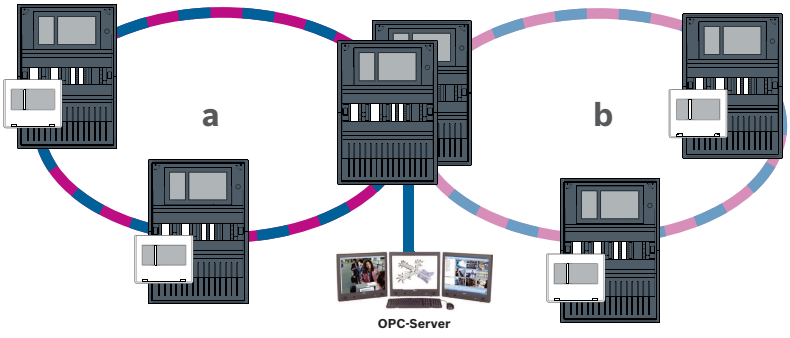
Parametry

– Serwer OPC może być podłączony za pośrednictwem kabla Ethernet (miedzianego) lub kabla światłowodowego.

W niniejszych przykładach pętla a jest siecią szkieletową. Pętla b jest podpętlą.



Rysunek 4.9: Podłączanie pętli Ethernet za pośrednictwem centrali nienadmiarowej



Rysunek 4.10: Podłączanie pętli Ethernet za pośrednictwem centrali nadmiarowej

5 Sieć Ethernet

W sieci połączenia Ethernet są monitorowane w sposób ciągły. W przypadku zerwania połączenia wykrywana jest przerwa. Wykrywane są również naprawione połączenia. Diagnostyka sieci danej centrali zawsze pokazuje adresy MAC hostów połączonych za pośrednictwem sieci.

Adresy MAC

W celu połączenia z siecią każdy kontroler centrali podaje następujące adresy MAC.

– Adres MAC hosta
– Adres MAC do identyfikacji portu ETH1
– Adres MAC do identyfikacji portu ETH2

W zależności od typu kontrolera centrali:

– Adres MAC do identyfikacji portu ETH3
– Adres MAC do identyfikacji portu ETH4

Zasady dotyczące używania 4 portów Ethernet

Jeśli Twoja centrala ma 4 porty Ethernet, zastosuj następujące reguły w podanej kolejności. Bosch obsługuje tylko sieci zbudowane zgodnie z poniższymi zasadami.

1. W celu połączenia centrali z siecią należy użyć ETH1 oraz ETH2. Zewnętrzny switch RSTP na ETH1 lub ETH2 może być używany tylko do połączenia centrali z siecią.
2. Do połączenia OPC, FSM-5000-FSI, Praesideo/PAVIRO, UGM-2040 należy użyć ETH3. Można podłączyć zewnętrzny switch RSTP, którego nie wolno używać do połączenia centrali z siecią.
3. W przypadku Remote Services należy użyć ETH4. Jeśli nie jest wymagane połączenie z Remote Services, wówczas można użyć ETH4 do połączenia OPC, FSM-5000-FSI, Praesideo/PAVIRO lub UGM-2040.
4. Jeśli nie żadna centrala nie jest połączona z siecią przez ETH1 i ETH2, wówczas każda można być używa do połączenia OPC, FSM-5000-FSI, Praesideo/PAVIRO lub UGM-2040.

5.1 Protokoły

SNMP

Protokół SNMP służy do monitorowania i kontrolowania składników sieciowych. Możliwy jest odczyt i modyfikowanie parametrów węzłów sieci. Wymaga to odpowiedniego oprogramowania do zarządzania siecią (np. Hirschmann HiVision).

Uwaga!
Sieć SNMP korzysta ze stałego ciągu identyfikacyjnego:PUBLIC

Uwaga: seria AVENAR panel nie obsługuje jeszcze protokołu SNMP.

LLDP

LLDP jest podstawowym protokołem zaprojektowanym na bazie standardów IEEE, który jest używany do udostępniania informacji sieciowych między sąsiednimi urządzeniami. Te informacje są

– dostarczane jako część danych SNMP i
– wyświetlane za pośrednictwem kontrolera centrali jako element danych dotyczących diagnostyki sieci.

RSTP

RSTP jest protokołem sieciowym zaprojektowanym na bazie standardów IEEE. RSTP zapewnia eliminowanie pętli w sieciach. Nadmiarowe ścieżki w sieci są wykrywane, dezaktywowane i aktywowane w razie potrzeby (awaria połączenia).
Dokładnie w tym celu protokół jest używany w sieci.
Zmiana w topologii magistrali w następstwie awarii połączenia jest automatycznie anulowana bezpośrednio po usunięciu awarii.

5.2 Średnica sieci

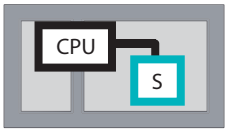
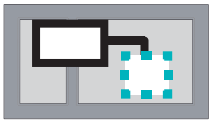
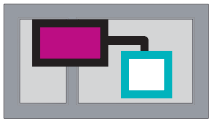
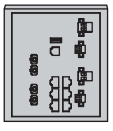
Średnica sieci RSTP Ethernet nie może być większa niż 32.

Definicja

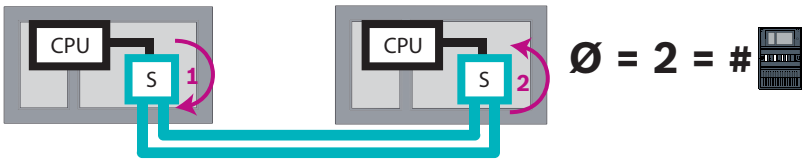
Średnica sieci odpowiada liczbie przełączników RSTP na najdłuższym możliwym odcinku bez pętli pomiędzy dowolnymi dwoma końcowymi punktami sieci.
Należy wziąć pod uwagę następujące kwestie dotyczące sieci RSTP Ethernet central:

- Każdy kontroler centrali zawiera punkt końcowy i wewnętrzny przełącznik RSTP.
- Połączenie kontrolera centrali i nadmiarowego kontrolera centrali liczy się jako jeden przełącznik RSTP.
- Konwertery transmisji nie są traktowane jako przełączniki RSTP.
- Najdłuższy możliwy odcinek nie może obejmować połączeń CAN.
- Serwery OPC nie są uwzględniane przy liczeniu średnicy sieci.

Klucz

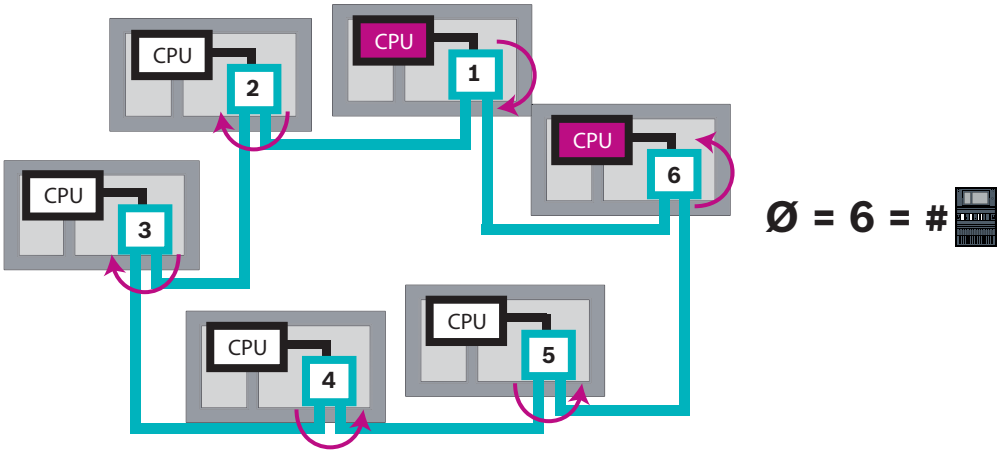
	Procesor główny w kontrolerze centrali lub w zdalnej klawiaturze.
	Wewnętrzny przełącznik RSTP w kontrolerze centrali lub w zdalnej klawiaturze.
	Kontroler centrali lub zdalna klawiatura z procesorem głównym i wewnętrznym przełącznikiem RSTP.
	Nadmiarowy kontroler centrali z procesorem głównym i wewnętrznym przełącznikiem RSTP
	Kontroler centrali lub zdalna klawiatura Punkt początkowy lub punkt końcowy służący do określania średnicy sieci w przykładach
	Przełącznik sieci Ethernet jako zewnętrzny przełącznik RSTP (ogólnie przełącznik Ethernet MM)

Dwie połączone centrale tworzą najmniejszą możliwą pętlę. Średnica tej sieci równa się 2, ponieważ wewnętrzne przełączniki RSTP znajdują się pomiędzy końcowymi punktami.



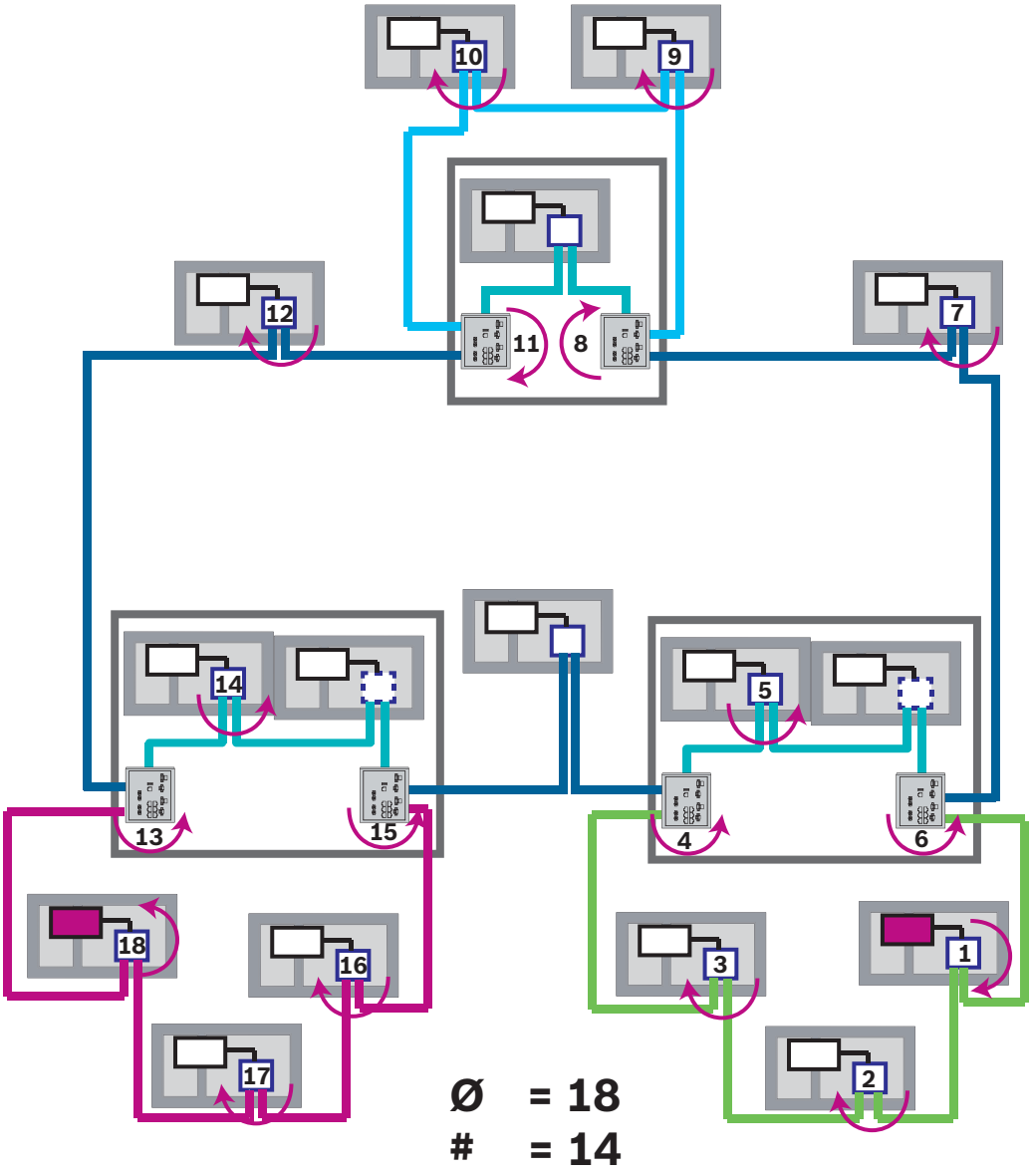
Rysunek 5.1: Pojemność sieci pętli z 2 centralami

W pętli central bez zewnętrznych przełączników RSTP średnica sieci odpowiada liczbie zainstalowanych central.



Rysunek 5.2: Średnica sieci pętli z 6 centralami

Jeśli sieć szkieletowa i podpętle są połączone ze sobą za pośrednictwem przełączników sieci Ethernet, to te zewnętrzne przełączniki RSTP należy również wziąć pod uwagę.



Rysunek 5.3: Średnica sieci szkieletowej z podpętlami

Aby określić średnicę sieci z tego rysunku, należy znaleźć najdłuższą trasę.

5.3 Stosowane kable

Instalacje sieciowe wymagają korzystania wyłącznie z następujących kabli. Stosowanie innych kabli jest niezgodne z normami bezpieczeństwa określonymi w dyrektywie WE.

– Kabel Ethernet
  Kabel sieciowy Ethernet, ekranowany, CAT 5e lub lepszy.
  Należy pamiętać o minimalnym promieniu zgięcia określonym w specyfikacji kabla.
– Kabel światłowodowy
  Wielofunkcyjny: kabel światłowodowy Ethernet krosowy, wtyczka dupleks I-VH2G 50/125µ lub dupleks I-VH2G 62.5/125µ, SC.
  Tryb pojedynczy: kabel światłowodowy Ethernet krosowy, wtyczka dupleks I-VH2E 9/125µ, SC.
  Należy pamiętać o minimalnym promieniu zgięcia określonym w specyfikacji kabla.

Uwaga!
Długość kabla TX
Wszystkie połączenia IP muszą być bezpośrednie lub poprzez konwertery transmisji zatwierdzone przez firmę Bosch. Długość kabla TX miedzy węzłami musi być mniejsza niż 100 m.

Uwaga!
VdS 2540
Aby spełnić wymagania dyrektywy VdS 2540, należy dla torów transmisji danych używać do połączeń Ethernet kabli światłowodowych. W przypadku połączeń w obudowie można użyć kabli Ethernet TX.

5.4 Tworzenie lub modyfikowanie sieci Ethernet

Istnieje kilka procedur w zakresie tworzenia sieci Ethernet central sygnalizacji pożaru. Opisane poniżej dwie procedury różnią się co do wielkości sieci i liczby wymaganych zadań związanych z instalacją i konfiguracją.

Zasady dotyczące używania 4 portów Ethernet

Jeśli Twoja centrala ma 4 porty Ethernet, zastosuj następujące reguły w podanej kolejności. Bosch obsługuje tylko sieci zbudowane zgodnie z poniższymi zasadami.

1. W celu połączenia centrali z siecią należy użyć ETH1 oraz ETH2. Zewnętrzny switch RSTP na ETH1 lub ETH2 może być używany tylko do połączenia centrali z siecią.
2. Do połączenia OPC, FSM-5000-FSI, Praesideo/PAVIRO, UGM-2040 należy użyć ETH3. Można podłączyć zewnętrzny switch RSTP, którego nie wolno używać do połączenia centrali z siecią.
3. W przypadku Remote Services należy użyć ETH4. Jeśli nie jest wymagane połączenie z Remote Services, wówczas można użyć ETH4 do połączenia OPC, FSM-5000-FSI, Praesideo/PAVIRO lub UGM-2040.
4. Jeśli nie żadna centrala nie jest połączona z siecią przez ETH1 i ETH2, wówczas każda można być używa do połączenia OPC, FSM-5000-FSI, Praesideo/PAVIRO lub UGM-2040.

Tworzenie sieci Ethernet (mniejsze projekty)

Niniejsza procedura jest przeznaczona do realizacji projektów wymagających zaangażowania niewielkiej grupy techników pracujących jednocześnie przy instalacji systemu sygnalizacji pożaru.

1. Zaplanuj sieć.
2. Utwórz sieć w programie FSP-5000-RPS i skonfiguruj ustawienia sieciowe.
3. Wydrukuj informacje o sieci i umieść je w bezpiecznym miejscu lub zapisz na komputerze przenośnym.
4. Zainstaluj centrale sygnalizacji pożaru i kable sieciowe, a następnie podłącz je do sieci.
5. Skonfiguruj ustawienia sieciowe dla poszczególnych central sygnalizacji pożaru bezpośrednio w urządzeniu sterującym zgodnie z wydrukiem.
6. Zresetuj każdą z central sygnalizacji pożaru w sieci, aby uaktywnić konfigurację sieciową.
7. Podłącz komputer z aplikacją do programowania FSP-5000-RPS do centrali sygnalizacji pożaru w sieci. Za pośrednictwem tej centrali sygnalizacji pożaru załaduj tę konfigurację do wszystkich pozostałych central w sieci. Centrale redundantne synchronizują konfigurację z centralami głównymi.
8. Wykonaj resetowanie, aby wyzerować oczekujące komunikaty o błędach. Napraw błędy.

Skonfiguruj ustawienia sieciowe w centralach sygnalizacji pożaru. To umożliwi zaprogramowanie innych central sygnalizacji pożaru w sieci za pośrednictwem jednej centrali.

Tworzenie sieci Ethernet (średnie i duże projekty)

Niniejsza procedura jest przeznaczona do realizacji projektów wymagających wykonania pewnej liczby zadań jednocześnie przez kilka zespołów. Ze względu na to, że wiele zadań wykonywanych w trakcie instalacji i konfiguracji wymaga ponownego uruchamiania centrali sygnalizacji pożaru, sieć jest uruchamiana dopiero w dalszej części procedury.

1. Zaplanuj sieć.
2. Utwórz konfigurację sieci bez urządzeń peryferyjnych za pomocą FSP-5000-RPS.
3. Wydrukuj informacje o sieci i umieść je w bezpiecznym miejscu lub zapisz na komputerze przenośnym.
4. Zainstaluj kable sieciowe i sprawdź poszczególne sekcje lub pętle.
5. Zainstaluj centrale i uruchom je jako urządzenia autonomiczne.
6. Zainstaluj urządzenia peryferyjne w centralach.
7. Skonfiguruj poszczególne centrale przy użyciu FSP-5000-RPS.
8. Upewnij się, że każda centrala działa prawidłowo.
9. Uruchom poszczególne pętle sieci jedną po drugiej, zgodnie z topologią.
   Uruchom sieć szkieletową.
   - Utwórz w FSP-5000-RPS konfigurację dotyczącą sieci szkieletowej. Importuj wszystkie potrzebne konfiguracje central. Skonfiguruj ustawienia sieciowe i wydrukuj je.
   - Podłącz wszystkie centrale do sieci.
   - Skonfiguruj ustawienia sieciowe dla poszczególnych central sygnalizacji pożaru bezpośrednio w kontrolerze centrali zgodnie z wydrukiem.
   - Zresetuj każdą z central sygnalizacji pożaru, aby załadować konfigurację sieciową.
   - Aby sprawdzić sieć, wyślij pakiety ping do sąsiednich central.
   - Uruchom całą sieć szkieletową i napraw ewentualne błędy.

   Uruchom podpętle zgodnie z przykładem sieci szkieletowej.

Dodawanie centrali do sieci

1. Zmień konfigurację sieci w FSP-5000-RPS.
2. Wydrukuj informacje o sieci i umieść je w bezpiecznym miejscu lub zapisz na komputerze przenośnym.
3. Zainstaluj centrale sygnalizacji pożarowej i kable sieciowe, a następnie podłącz je do sieci.
4. Skonfiguruj ustawienia sieciowe dla poszczególnych central sygnalizacji pożaru bezpośrednio w urządzeniu sterującym zgodnie z wydrukiem.
5. Zresetuj centralę i przyłączone centrale, aby uaktywnić konfigurację sieciową.

Usuwanie centrali z sieci

1. Zmień konfigurację sieci w FSP-5000-RPS.
2. Wydrukuj informacje o sieci i umieść je w bezpiecznym miejscu lub zapisz na komputerze przenośnym.
3. Skonfiguruj ustawienia sieciowe przyłączonych central sygnalizacji pożarowej bezpośrednio w urządzeniu sterującym zgodnie z wydrukiem.
4. Przed odłączeniem od sieci wyłącz zasilanie centrali (sieciowe i akumulatorowe).
5. Zresetuj przyłączone centrale, aby uaktywnić konfigurację sieciową.

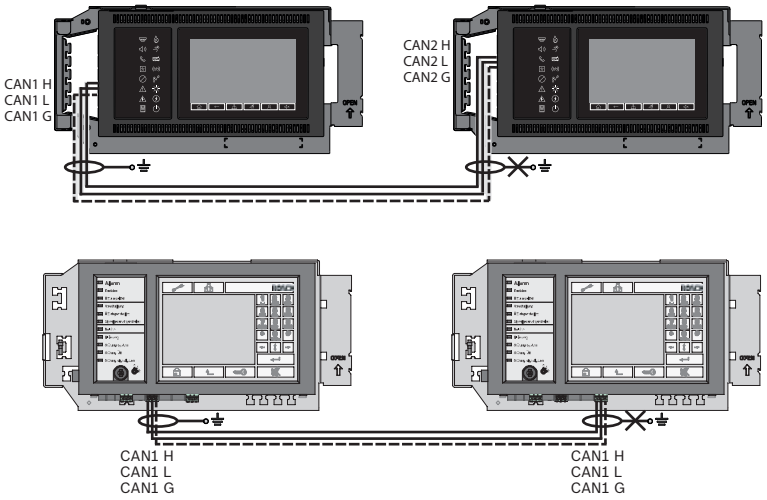
6 Sieć CAN

Topologia pętli

W topologii pętli kabel CAN zawsze prowadzi od terminalu CAN1 do terminalu CAN2 [CAN1 ⇒ CAN2]. długość kabla zależy od przekroju poprzecznego kabla.

Połączenie z siecią CAN

Połączenie CAN to połączenie dwużyłowe (CAN-H i CAN-L). Połącz CAN-H z CAN-H i połącz CAN-L z CAN-L, aby utworzyć połączenie z dwoma przewodami. W wyjątkowych przypadkach może być konieczne zastosowanie trzyżyłowego połączenia (CAN-H, CAN-L i CAN-GND), np. przy dużym obciążeniu EMC lub znaczącej różnicy potencjałów uziemienia. Połącz CAN-H z CAN-H, CAN-L z CAN-L i CAN-GND z CAN-GND, aby utworzyć połączenie z trzema przewodami. Ekranowany kabel CAN jest podłączony jedynie do metalowej obudowy z jednej strony.



Rysunek 6.1: Połączenie CAN (u góry: AVENAR, u dołu: FPA)

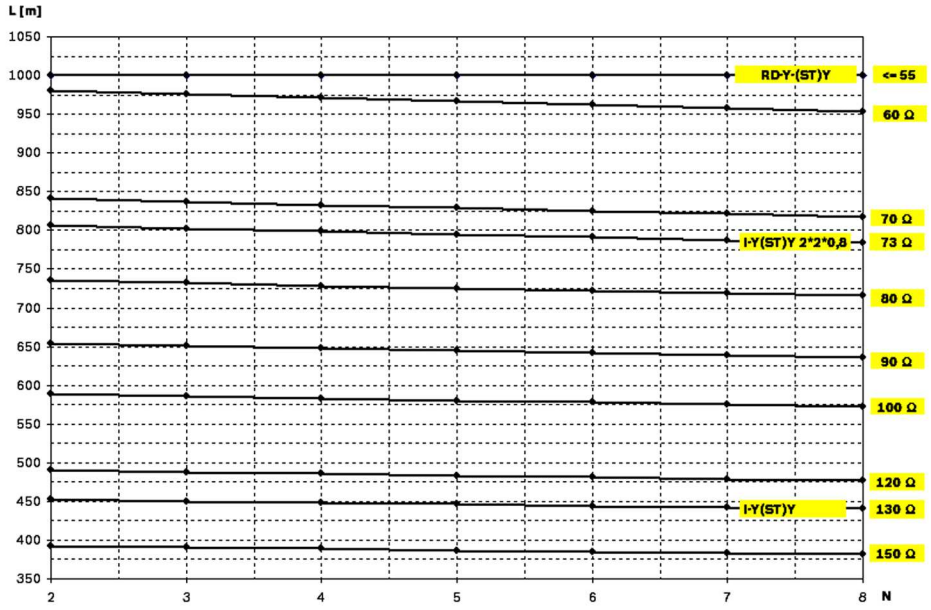
Długość kabla dla połączenia z siecią

Maksymalna dozwolona długość kabla zależy od rezystancji pętli użytego kabla i liczby komunikujących się węzłów.

Przykład: kabel czerwonej czujki pożarowej J-Y (St) Y 2 x 2 x 0,8 mm umożliwia połączenie dwóch węzłów, które dzieli maksymalnie 800 m.

Uwaga!

Odległość pomiędzy dwoma węzłami w topologii pętli można określić, odczytując wartość dwóch węzłów na diagramie.



Rysunek 6.2: Sieć CAN: dopuszczalna długość kabla jest zależna od liczby węzłów i oporności kabla

L = długość kabla w metrach

N = liczba węzłów

6.1 Tworzenie lub modyfikowanie sieci CAN

Niniejsza procedura jest przeznaczona do realizacji projektów wymagających zaangażowania niewielkiej grupy techników pracujących jednocześnie przy instalacji systemu sygnalizacji pożaru.

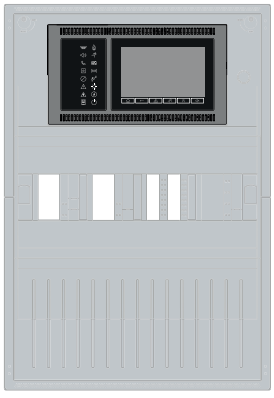
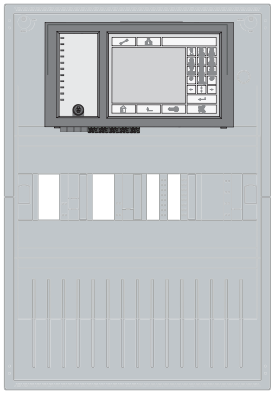
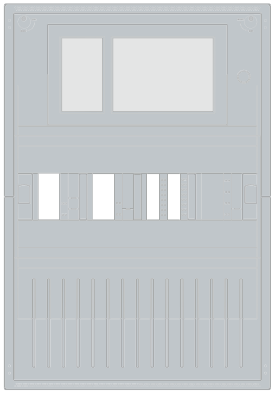
Procedura tworzenia sieci CAN

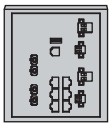
1. Zaplanuj sieć.
2. Utwórz sieć w FSP-5000-RPS.
3. Wydrukuj informacje o sieci i umieść je w bezpiecznym miejscu lub zapisz na komputerze przenośnym.
4. Zainstaluj centrale sygnalizacji pożaru i podłącz je kablami CAN do sieci.
5. Podłącz komputer z aplikacją do programowania FSP-5000-RPS do centrali sygnalizacji pożaru w sieci. Za pośrednictwem tej centrali sygnalizacji pożaru załaduj tę konfigurację do wszystkich pozostałych central w sieci. W nadmiarowych centralach stosowana jest konfiguracja głównej centrali.
6. Wykonaj resetowanie, aby wyzerować oczekujące komunikaty o błędach. Napraw błędy.

7 Schemat sieci Ethernet i CAN

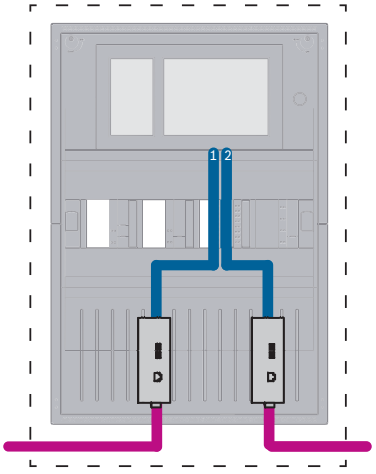
Aby utworzyć sieć centrali odpowiadającą wprowadzonej topologii i usługom łączności, wymagany jest schemat sieci opisany w tym dokumencie.

Ikona	Opis
	Kabel Ethernet TX (miedziany), długość kabla TX pomiędzy węzłami < 100 m
	Kabel Ethernet FX (kabel światłowodowy)

Ikona	Opis
	Kabel Ethernet TX lub FX, długość kabla TX pomiędzy węzłami < 100 m
	Kabel CAN
	Obudowa Uwaga: aby uprościć przegląd różnych wzorców połączenia z siecią, liczby w tym rozdziale pokazują zawsze małą obudowę centrali, która symbolizuje centralę. Ta mała obudowa **nie** zapewnia we wszystkich prezentowanych przypadkach wystarczającej ilości miejsca do zamontowania wyświetlanych switchów, konwerterów nośników oraz bram. Użyj Safety Systems Designer, aby zamówić prawidłowy rozmiar obudowy do zainstalowania wymaganego sprzętu.
	AVENAR panel
	FPA
	AVENAR panel lub FPA

Ikona	Opis
	Przełącznik sieci Ethernet jako zewnętrzny switch RSTP (ogólnie switch Ethernet MM)
	Konwerter transmisji
	Bezpieczna brama sieciowa usług Remote Services
	Połączenie z serwerem OPC, FSM-5000-FSI, Praesideo/PAVIRO lub UGM-2040

7.1 Łączenie central w sieć Ethernet



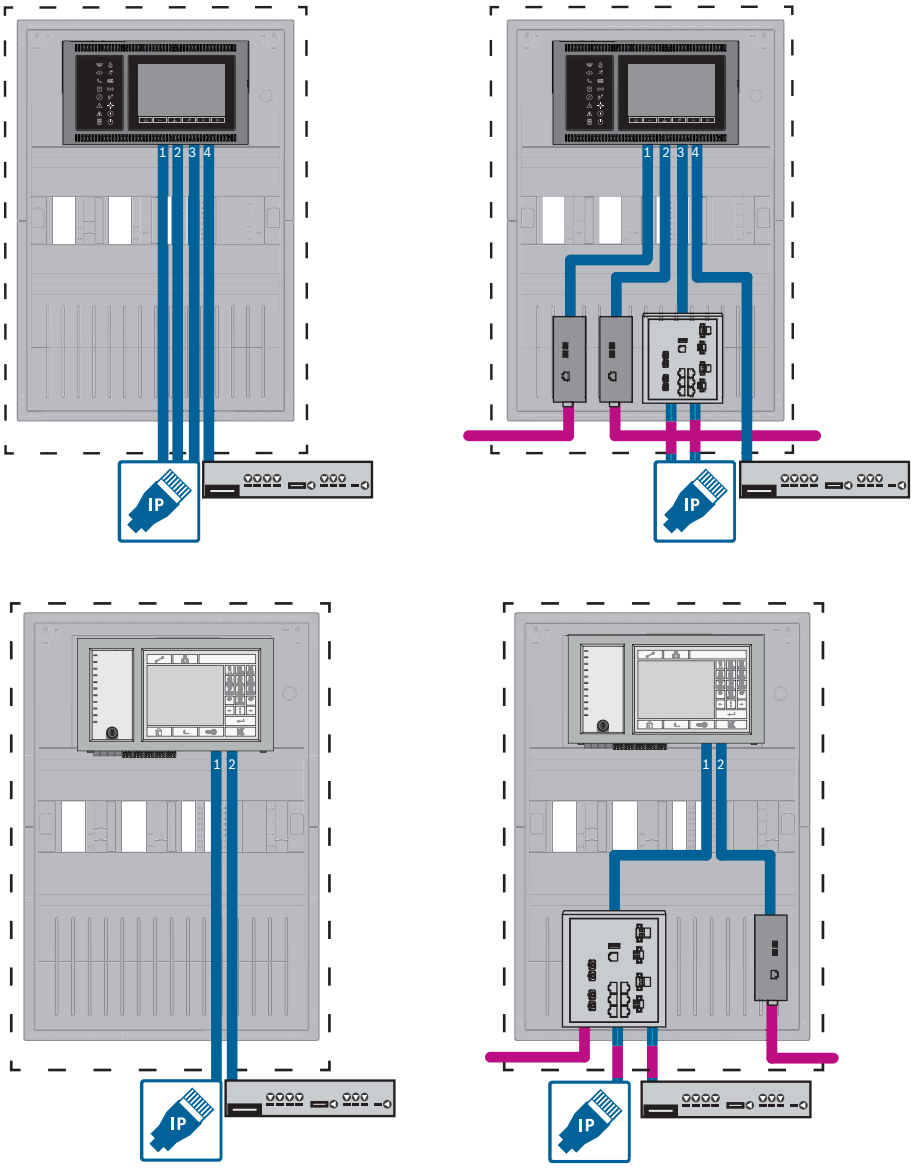
Rysunek 7.1: Łączenie central w sieć Ethernet

Dla odległości większych niż 100 m wymagane jest użycie konwerterów transmisji. Dla odległości mniejszych niż 100 użycie m konwerterów transmisji może nie być wymagane.

7.2 Łączenie central w sieć CAN

Rysunek 7.2: Łączenie central w sieć CAN

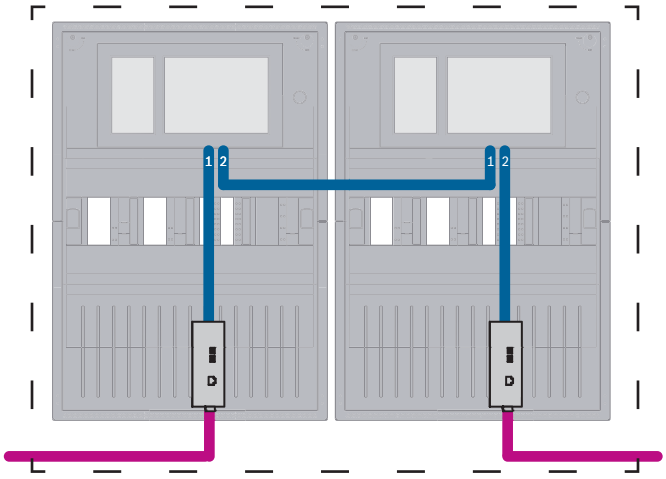
7.3 Podłączanie usług do centrali



Rysunek 7.3: Po lewej stronie: bez sieci central; po prawej stronie: z siecią central

Dla odległości większych niż 100 m wymagane jest użycie konwerterów transmisji. Dla odległości mniejszych niż 100 użycie m konwerterów transmisji może nie być wymagane.

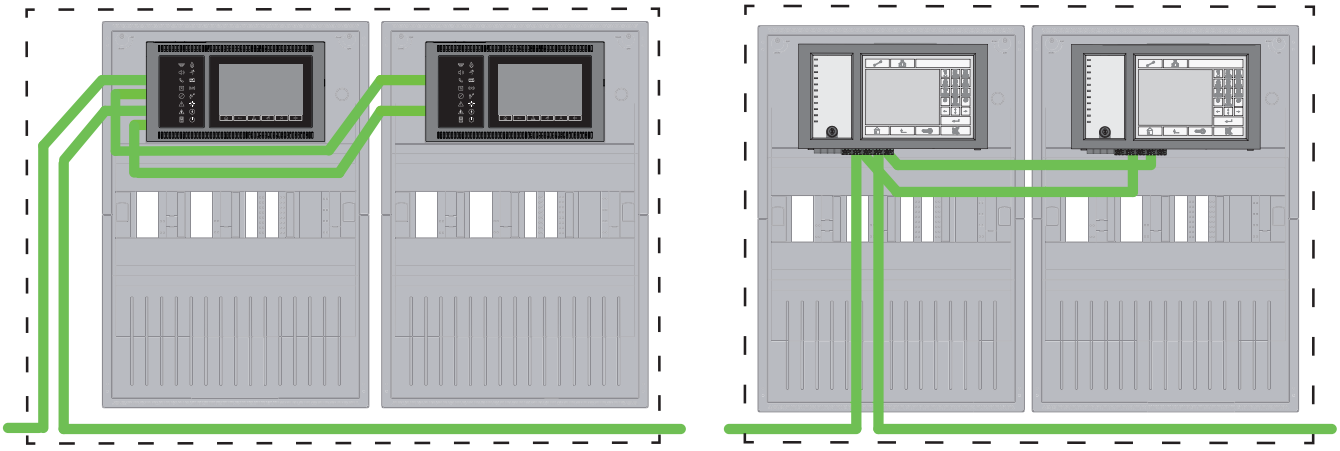
7.4 Sieć central w sieci Ethernet z centralami redundantnymi



Rysunek 7.4: Sieć central w sieci Ethernet z centralami redundantnymi

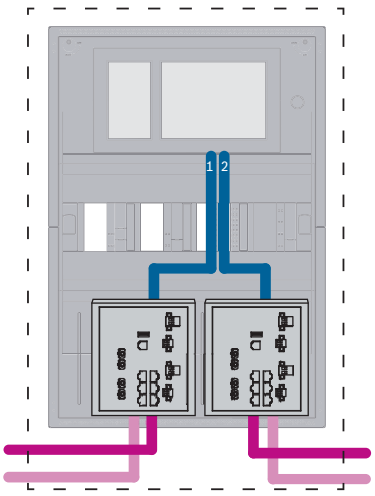
Dla odległości większych niż 100 m wymagane jest użycie konwerterów transmisji. Dla odległości mniejszych niż 100 użycie m konwerterów transmisji może nie być wymagane.

7.5 Sieć central w sieci CAN z centralami redundantnymi



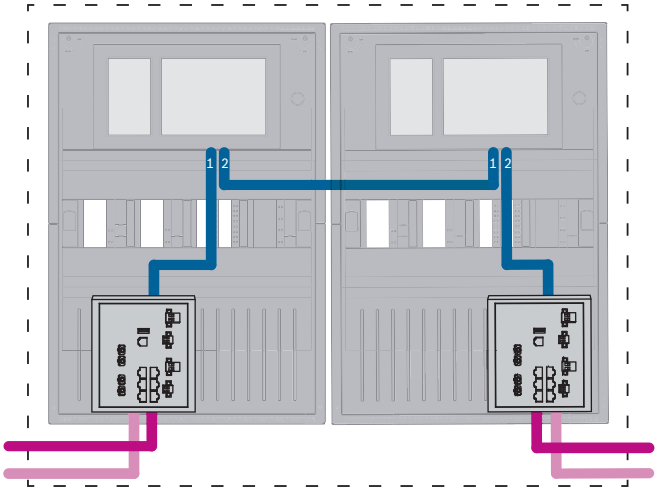
Rysunek 7.5: Sieć central w sieci CAN z centralami redundantnymi

7.6 Połączenie centrali z siecią za pomocą dwóch pętli sieci Ethernet



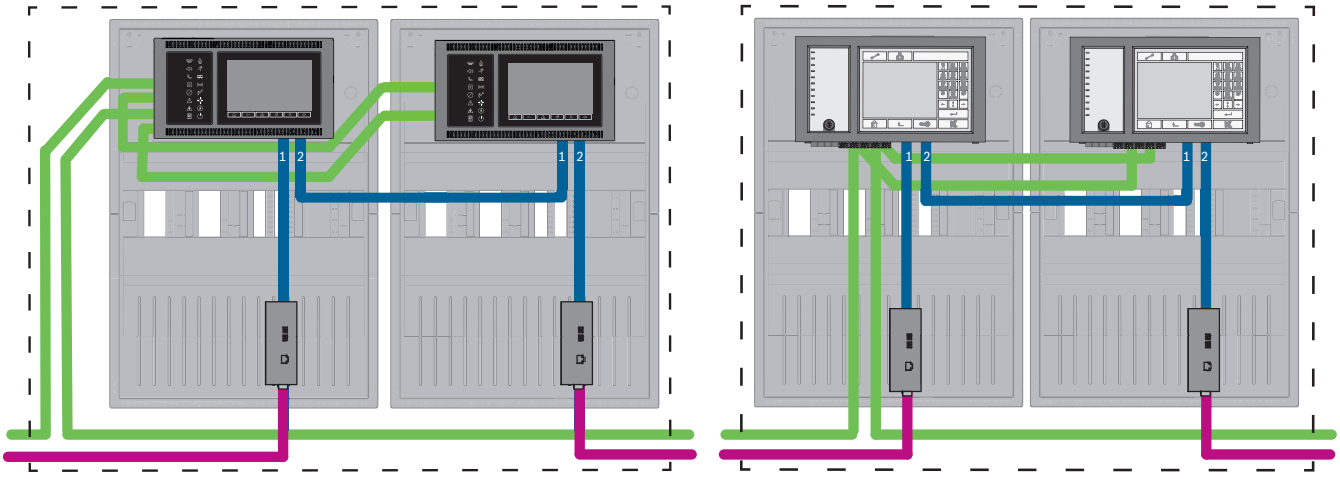
Rysunek 7.6: Połączenia sieci Ethernet

7.7 Sieć central w dwóch pętlach sieci Ethernet z centralami redundantnymi



Rysunek 7.7: Połączenia sieci Ethernet z centralami redundantnymi

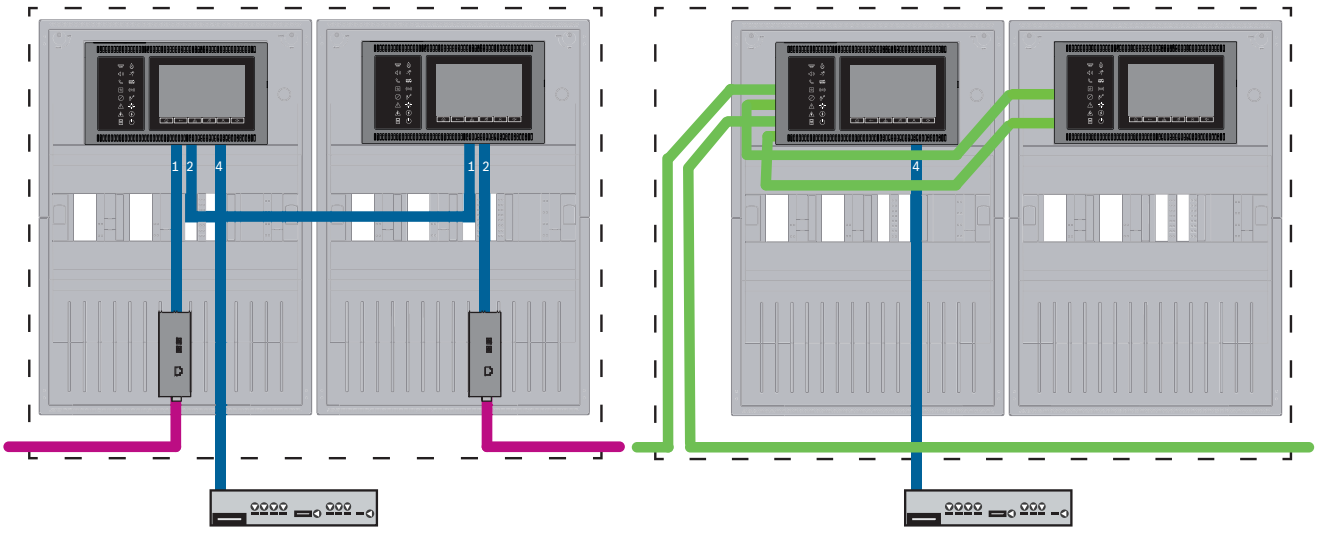
7.8 Połączenia sieci Ethernet i CAN z centralami redundantnymi

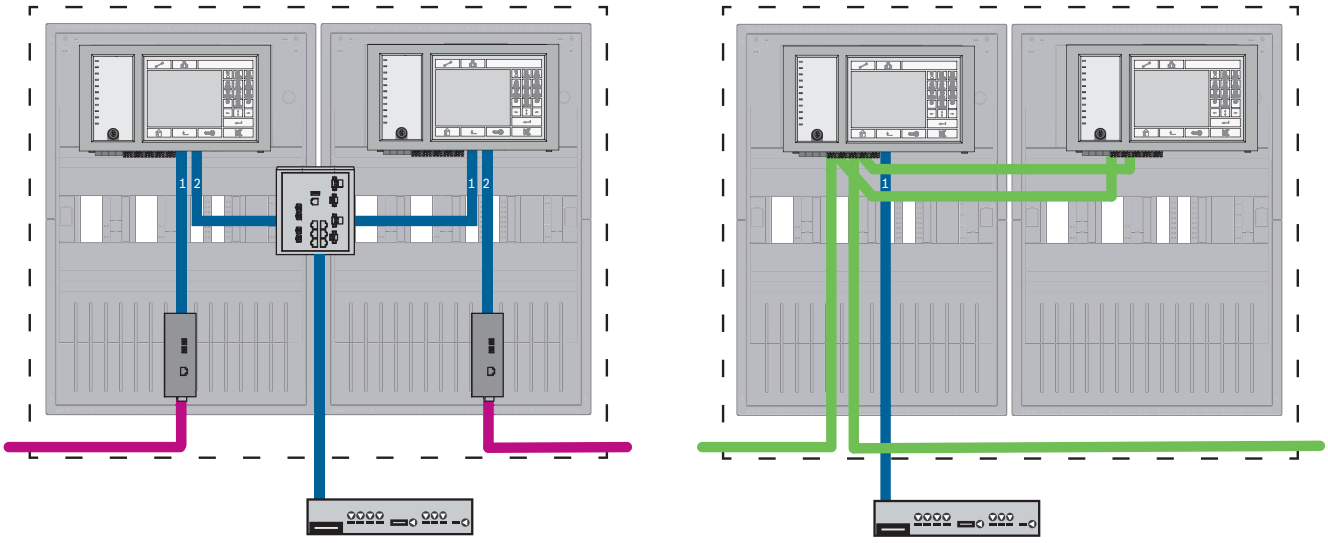


Rysunek 7.8: Połączenia sieci Ethernet i CAN z centralami redundantnymi

Dla odległości większych niż 100 m wymagane jest użycie konwerterów transmisji. Dla odległości mniejszych niż 100 użycie m konwerterów transmisji może nie być wymagane.

7.9 Podłączanie usług zdalnych do central redundantnymi





Rysunek 7.9: Po lewej stronie: sieć Ethernet; po prawej stronie : sieć CAN

Dla odległości większych niż 100 m wymagane jest użycie konwerterów transmisji. Dla odległości mniejszych niż 100 użycie m konwerterów transmisji może nie być wymagane.

8 Usługi Remote Services

Do Remote Services należą następujące usługi:

- Remote Connect
- Remote Alert
- Remote Maintenance

Warunkiem wstępnym dla usług Remote Alert i Remote Maintenance jest Remote Connect.

8.1 Remote Connect

Usługa Remote Connect zapewnia zaufane i bezpieczne połączenie internetowe, które umożliwia zdalny dostęp do centrali poprzez FSP-5000-RPS. Remote Connect jest podstawą dla Remote Services. Do połączeń Remote Connect należy używać bezpiecznej bramy sieciowej.

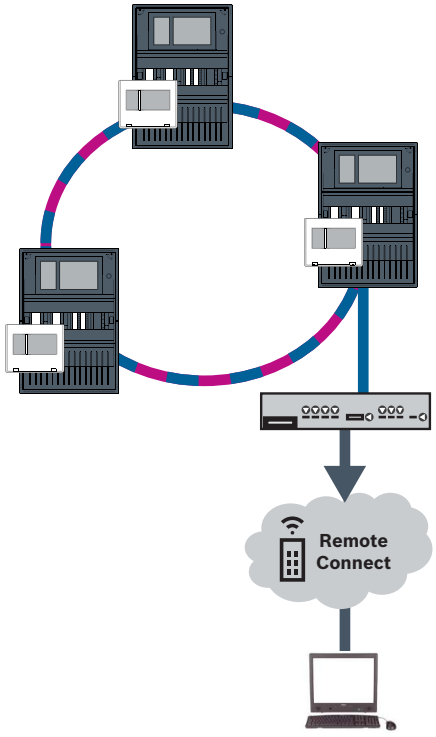
W przypadku sieci central jedna z centrali w sieci musi być podłączona do bezpiecznej bramy sieciowej. Tylko to połączenie musi być dedykowanym połączeniem Ethernet.

Uwaga!

Jeśli Remote Connect jest połączeniem do sieci central za pośrednictwem sieci Ethernet lub CAN, to funkcjonalność Remote Alert oraz Remote Maintenance jest obsługiwana tylko wtedy, gdy połączenie Ethernet pomiędzy centralami jest skonfigurowane do użytku z usługami.

Usługa Remote Connect musi być włączona w konfiguracji FSP-5000-RPS tej centrali.

Poniższa topologia przedstawia połączenie kontrolerów central w sieci Ethernet, gdzie bezpieczna brama sieciowa jest podłączona do sieci za pośrednictwem przełącznika Ethernet (ogólnie MM).



Rysunek 8.1: Usługa Remote Connect w pętli Ethernet

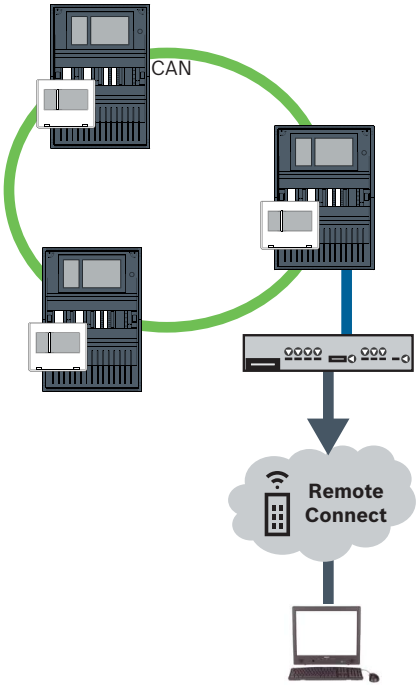
Uwaga!
Aby podłączyć centrale za pośrednictwem FX, należy użyć konwerterów transmisji zatwierdzonych przez firmę Bosch.

Aby uniemożliwić przesyłanie ruchu multiemisji zgodnego z normą EN 54-2 do routera, należy użyć przełącznika Ethernet (ogólnie MM, BPA-ESWEX-RSR20) przeznaczonego do obsługi centrali w wersji 2.8. Włącz śledzenie IGMP przełącznika Ethernet. Zobacz odpowiednią część w rozdziale dotyczącym instalacji, w instrukcji połączeń z siecią.

Uwaga!
Router internetowy (lub sieć firmowa zapewniająca dostęp do Internetu), a także bezpieczna brama sieciowa, muszą być oddzielone podsieciami. Centrale sieciowe nie mogą znajdować się w jednej podsieci z routerem internetowym. Nie jest również możliwe nakładanie się na siebie podsieci.
Jeśli podsieci się na siebie nakładają, trzeba je oddzielić, zmieniając adresy IP po stronie sieci centrali.
Ponadto należy rozszerzyć te zmiany na bezpieczną bramę sieciową. W tym celu należy uruchomić interfejs za pomocą przeglądarki internetowej:
- Adres: https://192.168.1.254
- Nazwa użytkownika: bosch
- Hasło: ipti83
Adres IP można zmienić w menu **Konfiguracja** -> **Sieć (LAN)**. Należy pamiętać, że adres bramy **Brama domyślna:** w konfiguracji kontrolera centrali musi być zgodny z adresem IP bezpiecznej bramy sieciowej.

Uwaga!
Zgodnie ze wskazówkami DIBt zdalne resetowanie nie jest dozwolone za pośrednictwem usług zdalnych w celu przywrócenia gotowości operacyjnej systemów sterowania drzwiami z silnikiem wspomagania otwierania.

Poniższa topologia pokazuje sieć CAN, w której bezpieczna brama sieciowa jest podłączona do sieci za pośrednictwem portu Ethernet.



Rysunek 8.2: Remote Connect w pętli CAN

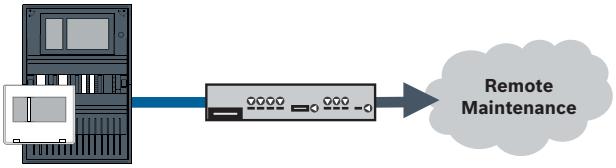
8.2 Remote Alert

Za pomocą alertu Remote Alert centrala przesyła informacje o stanie do portalu Remote Portal.
Transferowane dane są analizowane wraz z alertem Remote Alert. W przypadku nieoczekiwanego zdarzenia użytkownik zostanie poinformowany za pośrednictwem wiadomości SMS i/lub e-mail o otrzymanych alertach.

Usługa Remote Alertjest również dostępna w sieci Private Secure Network.

8.3 Usługa Remote Maintenance

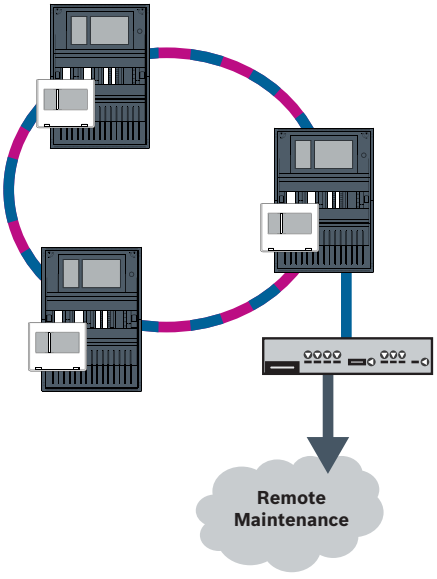
Remote Maintenance zapewnia możliwość zdalnego monitorowania określonych parametrów różnych elementów zabezpieczeń podłączonych do centrali sygnalizacji pożaru. Za pomocą usługi Remote Portal można wykonać obchód testowy.



Rysunek 8.3: Usługa Remote Maintenance

Uwaga!
W przypadku połączeń Ethernet używanych wyłącznie do przesyłania danych Remote Maintenance można korzystać z połączeń przy użyciu kabli Ethernet i światłowodowych. Należy pamiętać o maksymalnych dozwolonych długościach kabli.

Uwaga!
Aby podłączyć centrale za pośrednictwem FX, należy użyć konwerterów transmisji zatwierdzonych przez firmę Bosch.



Rysunek 8.4: Usługa Remote Maintenance

W przypadku korzystania z usługi Remote Maintenance w sieci Ethernet jedna centrala w sieci musi być podłączona do routera, aby umożliwić transfer danych. Wszystkie gromadzone dane są przesyłane z sieci za pośrednictwem tego połączenia.

Usługa Remote Maintenance dla Remote Portal

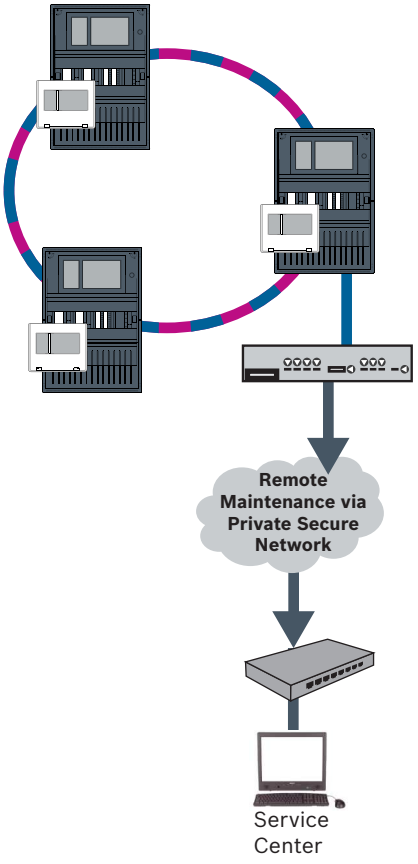
Remote Maintenance zbiera dane z odpowiednich urządzeń LSN i modułów funkcyjnych i przesyła je do Remote Portal, gdzie są one analizowane i wizualizowane w celu przeprowadzenia czynności konserwacyjnych.

Usługa Remote Maintenance dla sieci Private Secure Network

Remote Maintenance można także skonfigurować dla sieci Private Secure Network: gromadzone dane będą przesyłane do systemu centralnego serwera zarządzania (CMS).

Przestroga!
Usługi Remote Serviceswymagają bezpiecznego połączenia IP. Wymagane jest połączenie z BoschRemote Services lub Private Secure Network.
Z usługą Private Secure Network udostępniana jest sieć IP poprzez DSL z opcjonalnym bezprzewodowym dostępem z centrali (EffiLink). Remote Services do sieci Private Secure Network jest dostępna tylko w Niemczech na podstawie umowy o świadczenie usług z Bosch BT-IE.

Uwaga!
Aby podłączyć centrale za pośrednictwem FX, należy użyć konwerterów transmisji zatwierdzonych przez firmę Bosch.



Rysunek 8.5: Usługa Remote Maintenance dla sieci Private Secure Network

W przypadku usługi Remote Maintenance trzeba wprowadzić adres IP serwera i port serwera systemu Remote Maintenance w aplikacji do programowania FSP-5000-RPS.
Należy przypisać unikatowy identyfikator sieci central do sieci.

Przełącznik do podłączania systemu CMS musi być zaprogramowany oddzielnie.
Aby uzyskać informacje o programowaniu ustawień adresu IP i nadmiarowości przełącznika, patrz *Ustawienia przełącznika, Strona 45*. Ze względu na to, że przełącznik jest instalowany w bezpośrednim sąsiedztwie (bez wolnej przestrzeni), nie jest konieczne projektowanie nadmiarowego zasilania. Dlatego też wyjścia sygnału awarii nie są używane.
Należy upewnić się, że ustawienia RSTP w kontrolerach central, aplikacji do programowania FSP-5000-RPS i przełączniku Ethernet są identyczne.

8.4 Remote Portal

Wymagania

Uwaga!
Aby uniknąć ponownej konfiguracji lub regulacji, używając funkcji Remote Services, upewnij się, że są spełnione następujące wymagania:
- centrala z oprogramowaniem sprzętowym w wersji 2.19.7 lub nowszej, wszystkie centrale połączone za pośrednictwem sieci Ethernet, interfejsy Ethernet włączone, a ustawienia sieci Ethernet standardowe;
- Remote Connect włączone w konfiguracji centrali FSP-5000-RPS;
-Bezpieczna Brama sieciowa do Remote Services dostępna
- komputer z aplikacją do programowania FSP-5000-RPS w wersji 4.8 lub wyższej i dostępem do Internetu.

Uwaga!
Należy unikać aktualizacji bezpiecznej bramy sieciowej podczas połączenia.
Uruchamiaj aktualizacje bezpiecznej bramy sieciowej regularnie we wczesnych godzinach rannych. W tym celu określ strefę czasową, wybierając w menu **System** -> **General Settings** -> **Timezone**.

Konstrukcje

Aby używać usług Remote Services, trzeba być użytkownikiem konta Remote Portal.

Krok 1: Utwórz konto Remote Portal

Do konta Remote Portal może być przypisanych wielu użytkowników. Każde konto Remote Portal ma jeden niepowtarzalny identyfikator Remote ID, który jest przeznaczony dla jednej firmy. Jeśli nie można używać istniejącego konta Remote Portal, należy utworzyć nowe:

1. Na stronie https://remote.boschsecurity.com -> **Sign Up** (Załóż konto) wpisz imię i nazwisko, nazwę firmy oraz adres e-mail i utwórz hasło. Przeczytaj warunki korzystania z usługi i zaznacz **I agree to terms and conditions** (Akceptuję warunki korzystania z usługi). Przeczytaj także zasady ochrony prywatności i zaznacz **I agree to the privacy statement** (Akceptuję zasady ochrony prywatności).
2. Kliknij **Register** (Zarejestruj).
   Remote Portal natychmiast wyśle wiadomość e-mail z łączem aktywacyjnym na podany adres.
3. Aby aktywować konto, kliknij łącze aktywacyjne. W Remote Portal kliknij swoją nazwę użytkownika i wybierz **Account Settings** (Ustawienia konta). Tutaj znajdziesz swój identyfikator Remote ID. Identyfikator Remote ID będzie potrzebny w kontrolerze centrali na późniejszym etapie.

Aby zapewnić oddzielne konta dla techników, można utworzyć kilku użytkowników dla tego samego identyfikatora Remote ID:
Zaloguj się do Remote Portal.

- Wybierz **Users** (Użytkownicy) -> **New Technician** (Nowy technik). Następnie wpisz wymagane dane i potwierdź za pomocą przycisku **Save** (Zapisz).

Krok 2: Podłącz bezpieczną bramę sieciową

W celu utworzenia Remote Services użyj bezpiecznej bramy sieciowej.

1. Podłącz port WAN bezpiecznej bramy sieciowej do routera internetowego lub sieci firmowej z dostępem do Internetu.

2. Na ruterze internetowym lub w sieci firmowej sprawdź dostępność następujących protokołów i portów do bezpiecznej bramy sieciowej (wymaganych do połączenia z Remote Services).

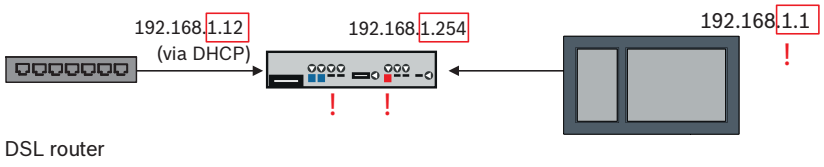
Protokół	Domyślny port	Opis
HTTP	80 i 8080	do rejestracji Remote Connect i Remote Maintenance
IPsec VPN	UDP 500 i UDP 4500	do Remote Connect

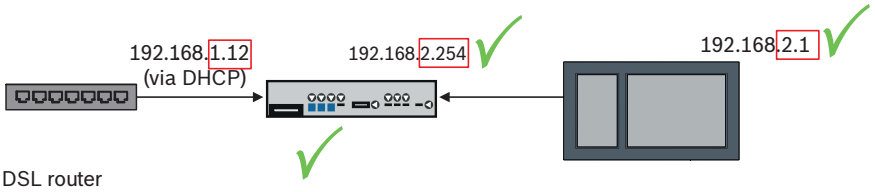
3. Podłącz port bezpiecznej bramy sieciowej LAN1 do odpowiedniego portu Ethernet kontrolera centrali za pomocą dołączonego kabla sieciowego CAT5 RJ45. Zauważ możliwe topologie.
4. Podłącz bezpieczną bramę sieciową do zasilania sieciowego 100 V - 230 V za pomocą zasilacza.

Po nawiązaniu połączenia z Internetem dioda LED WAN świeci na niebiesko. Wkrótce potem na niebiesko zaczyna świecić dioda LED VPN, co oznacza, że zostało nawiązane połączenie VPN z Remote Portal.
Każda dołączona centrala lub sieć central ma jeden niepowtarzalny identyfikator System ID.

Rozdzielanie podsieci (dioda LED VPN wył.)

Podłączenie bezpiecznej bramy sieciowej dla Remote Services nie powiedzie się w przypadku nakładających się podsieci (dioda LED VPN wył.). Poniższy przykład przedstawia bezpieczną bramę sieciową i kontroler centrali znajdujące się w tym samym zakresie adresów co router DSL.





Bezpieczna brama sieciowa z najnowszym oprogramowaniem sprzętowym wykrywa jednoznacznie nakładające się podsieci: dioda LED Alarm miga w sposób ciągły.
Aby rozdzielić podsieci, należy zmienić trzeci oktet adresu IP. Adresy IP można zmienić po stronie sieci centrali. Po zmianie adresu IP należy zastosować zmiany w bezpiecznej bramie sieciowej. W tym celu należy uruchomić interfejs za pomocą przeglądarki internetowej:
- Adres: https://192.168.1.254
- Nazwa użytkownika: bosch

- Hasło: ipti83

W menu **Konfiguracja** -> **Sieć (LAN)** można zmienić adres IP. Należy pamiętać, że adres bramy **Brama domyślna:** w konfiguracji kontrolera centrali musi być zgodny z adresem IP bezpiecznej bramy sieciowej.

Krok 3: Nawiąż połączenie zdalne

1. W centrali użyj standardowych ustawień sieci Ethernet.
2. Zrestartuj centralę.
3. Do uwierzytelnienia wybierz **Configuration** -> **Network Services** -> **Change date / time** (Konfiguracja -> Usługi sieciowe -> Zmień datę/godzinę), wpisz bieżącą datę i potwierdź ustawienia.
4. Wybierz **Configuration** -> **Network Services** -> **Remote Services** (Konfiguracja -> Usługi sieciowe -> Remote Services), a następnie wpisz identyfikator Remote ID.

Można sprawdzić stan zdalnego połączenia: wybierz **Diagnostics** -> **Network Services** -> **Remote Services** (Diagnostyka -> Usługi sieciowe -> Remote Services) na kontrolerze centrali.

Krok 4: Przypisz licencję w Remote Portal

Aby aktywować usługę Remote Services, należy przypisać licencję do Remote Portal. Jedna licencja jest dostarczana automatycznie do danego konta przy pierwszym udanym połączeniu.

Uwaga!
Raz przypisanej licencji nie da się przypisać ponownie ani zawiesić.

1. Na stronie https://remote.boschsecurity.com -> **Login** (Zaloguj się), wpisz swój adres e-mail i hasło.
2. Wybierz **Systems** (Systemy).
3. Wybierz system.
4. W obszarze **Services** (Usługi) kliknij przycisk **Add Service** (Dodaj usługę) pod usługą.
5. Domyślnie licencja będzie automatycznie odnawiania (**Service Settings** (Ustawienia usługi), opcja **With Auto-Renew** (Z automatycznym odnawianiem)).
6. Kliknij przycisk **Save** (Zapisz), aby potwierdzić ustawienia.

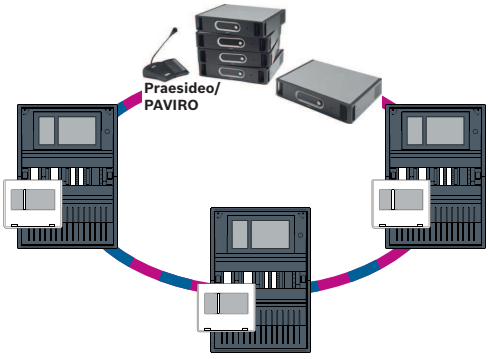
Po przypisaniu licencji można korzystać z odpowiedniej usługi. Przypisana licencja jest oznaczona zielonym haczykiem.

Krok 5: Zamów ponownie licencję

1. Zamów jednoroczne licencje w Bosch Fire Alarm Systems. Każda sieć wymaga własnej licencji. Firma
   Bosch wyśle wiadomość e-mail na podany adres. W wiadomości znajdują się niepowtarzalne numery do zarejestrowania zamówionych licencji, a także instrukcje i łącze do Remote Portal.
2. Na stronie https://remote.boschsecurity.com -> **Login** (Zaloguj się), wpisz swój adres e-mail i hasło.
3. Wybierz **Licenses** (Licencje).
4. Kliknij przycisk **+**.
5. Postępuj zgodnie z instrukcjami wyświetlonymi w oknie **Add Licenses** (Dodaj licencje) i potwierdź, klikając przycisk **Save** (Zapisz).
6. Lista licencji zostanie zaktualizowana.

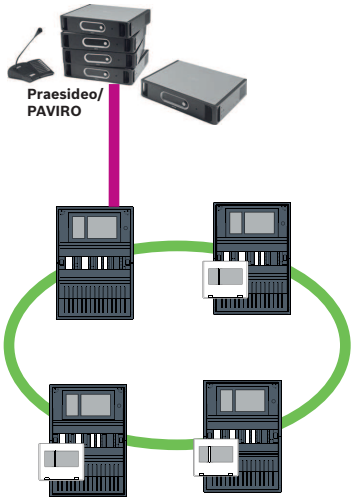
9 Dźwiękowe systemy ostrzegawcze

Poniższa topologia przedstawia połączenie kontrolerów central poprzez Ethernet, gdzie system Praesideo/PAVIRO jest zintegrowany w pętli central za pomocą interfejsu Ethernet.



Rysunek 9.1: Pętla Ethernet z Praesideo/PAVIRO

Należy użyć przełącznika Ethernet Switch (zasadniczo MM BPA-ESWEX-RSR20) przeznaczonego do obsługi oprogramowania sprzętowego centrali w wersji 2.8.
Aby uniemożliwić przesyłanie ruchu multicastowego zgodnego z normą EN 54-2 do systemu Praesideo/PAVIRO, należy aktywować śledzenie IGMP z MM. Zobacz odpowiednią część w rozdziale dotyczącym instalacji, w instrukcji połączeń z siecią.
W każdym kontrolerze centrali sieci CAN można podłączyć jeden system Praesideo/PAVIRO za pomocą interfejsu Ethernet. Poniższa topologia przedstawia połączenie kontrolerów centrali poprzez CAN, gdzie system Praesideo/PAVIRO jest podłączony do jednego kontrolera za pomocą interfejsu sieci Ethernet.



Rysunek 9.2: Połączenie Praesideo/PAVIRO z siecią CAN

Uwaga!
Ruch w sieci CAN nie powinien odbywać się poprzez połączenie Ethernet, dlatego należy wyłączyć połączenie z siecią poprzez IP w aplikacji do programowania FSP-5000-RPS. Jeśli ta funkcja nie zostanie wyłączona, sieć nie będzie zgodna z normą EN 54.

Uwaga!
Jeśli kontroler centrali MPC-xxxx-B ma służyć do bezpośredniego połączenia z systemem Praesideo/PAVIRO, wymagane jest użycie połączeniowego kabla krosowego, ponieważ ani Praesideo/PAVIRO, ani MPC-xxxx-B nie obsługują Auto-MDI(X).

10 Instalacja

Lista kontrolna

Przed rozpoczęciem instalacji sieci należy sprawdzić wszystkie poniższe punkty.

– Ethernet i CAN

  - Wymagane długości kabli Ethernet TX, Ethernet FX, CAN TX oraz CAN FX są mniejsze od ich długości maksymalnych.
  - Zaplanowano wszystkie urządzenia peryferyjne i ich okablowanie w poszczególnych centralach.
- Planowanie sieci
  - Wszystkie ustawienia adresów IP i sieciowe dla poszczególnych central oraz dodatkowe składniki sieciowe są zaplanowane i do dyspozycji.
  - Sprawdzono, czy do dyspozycji są dodatkowe składniki, które mają być zainstalowane, takie jak przełączniki Ethernet i konwertery transmisji, oraz ich okablowanie z sąsiednimi centralami.
  - Sprawdzono, czy do dyspozycji jest topologia sieci, która ma być zainstalowana.
  - Wszystkie ustawienia nadmiarowości sieci są zaplanowane i do dyspozycji.

10.1 Ustawienia konwertera transmisji

Użycie konwertera transmisji wymaga wykonania tylko kilku czynności:
- Ustaw przełączniki DIP.
- Podłącz konwerter transmisji do kabli sieciowych FX i CAT5e.
- Podłącz konwerter transmisji do zasilania za pośrednictwem wewnętrznego modułu kontrolera akumulatorów BCM.

Uwaga!
Konwertery transmisji są zasilane wyłącznie za pośrednictwem końcówki nr 1 zasilacza.
Z tego powodu dioda błędu na konwerterze świeci w sposób ciągły. Nie ma to jednak wpływu na działanie urządzenia.

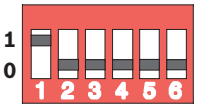
Uwaga!
Instalacje sieciowe wymagają korzystania wyłącznie z następujących kabli:
Kabel Ethernet
Kabel sieciowy Ethernet, ekranowany, CAT5e lub lepszy.
Należy pamiętać o minimalnym promieniu zgięcia określonym w specyfikacji kabla.
Kabel światłowodowy
Tryb multi-mode: sieciowy kabel światłowodowy Ethernet, dupleks I-VH2G 50/125µ lub dupleks I-VH2G 62.5/125µ, wtyczka SC.
Tryb pojedynczy: sieciowy kabel światłowodowy Ethernet, dupleks I-VH2E 9/125µ
Należy pamiętać o minimalnym promieniu zgięcia określonym w specyfikacji kabla.

Uwaga!
Więcej informacji o instalowaniu konwerterów transmisji w obudowach centrali: FPM 5000 KMC(F.01U.266.845)FPM-5000-KES(F.01U.266.844)

Uwaga!
W przypadku wielomodowych konwerterów transmisji maksymalna długość odcinka transmisji za pośrednictwem FX wynosi 2000 m.
W przypadku jednomodowych konwerterów transmisji maksymalna długość odcinka transmisji za pośrednictwem FX wynosi 40 km.

Za pomocą przełączników DIP należy skonfigurować konwerter transmisji, jak pokazano na poniższym rysunku.

Uwaga!
Zmiany ustawień przełącznika DIP w konwerterach transmisji mogą być wykonywane wyłącznie po odłączeniu zasilania.



Numer przełącznika DIP	Ustawienie
1	Aktywny tryb LFP (Link Fault Pass-Through)
2	Ethernet: tryb automatyczny
3	Ethernet: 100 MBit
4	Ethernet: pełny dupleks
5	Kabel światłowodowy: pełny dupleks
6	Awaria połączenia: wyłączone

10.2 Montaż przełącznika Ethernet

Ostrzeżenie!
Światło lasera
Nie należy patrzeć wprost na wiązkę nieuzbrojonym okiem ani przez przyrządy optyczne dowolnego rodzaju (np. przez szkło powiększające lub mikroskop). Zlekceważenie tego zalecenia jest niebezpieczne dla oczu, zwłaszcza przy odległościach mniejszych niż 100 mm. Wiązka świetlna jest obecna w terminalach optycznych i na końcach podłączonych do nich kabli światłowodowych. Dioda laserowa CLASS 2M, długość fali 650 nm, wydajność < 2 mW, zgodnie z normą IEC 60825-1.

Uwaga!
Patrz: Instrukcja instalacji zestawu montażowego przełącznika Ethernet FPM-5000-KES(F.01U.260.523).

10.3 Ustawienia przełącznika

Aby umożliwić użycie przełączników w sieci, trzeba je zaprogramować.
Podłącz komputer przenośny do sieci i za pomocą dostarczonego przez producenta oprogramowania HiDiscovery wykonaj wstępne programowanie przełączników. Posługując się tym oprogramowaniem, wyszukaj przełączniki w sieci. Kliknij dwukrotnie przełącznik, aby go wybrać, i przypisz do niego adres IP.
Po wstępnym zaprogramowaniu adresu IP można za pomocą przeglądarki internetowej wywołać interfejs użytkownika umożliwiający konfigurację przełącznika.

Uwaga!
Dokładny opis instalacji i konfiguracji przełączników można znaleźć w instrukcji producenta.
Dane dostępowe:
Użytkownik: admin
Hasło: private

Za pomocą przeglądarki wywołaj interfejs użytkownika, aby wybrać ustawienia dla przełączników.
Skonfiguruj następujące ustawienia:
– *Przypisanie adresu IP, Strona 46*,
– *Programowanie ustawień nadmiarowości, Strona 46*.
Ponadto dostępne są ustawienia opcjonalne, np.:
– *Programowanie przekaźnika usterki, Strona 47*,
– *Programowanie monitoringu połączeń, Strona 48*,
– *Jak włączyć śledzenie IGMP, Strona 48*.

10.3.1 Przypisanie adresu IP

Uwaga!
Praktyczna wskazówka:
Jeśli konfiguracja sieciowa to umożliwia, w części adresów IP dotyczących urządzenia dla przełączników należy używać liczb większych niż 200 (xxx.xxx.xxx.200). Zapewni to lepsze odróżnienie od identyfikatora adresu IP hosta.
Przykład:
Przełącznik 192.168.1.201 jest przypisany do centrali o adresie IP 192.168.1.1.

Uwaga!
Dokładny opis instalacji i konfiguracji przełączników można znaleźć w następujących dokumentach producenta:
Instrukcja instalacji
Skrócony przewodnik interfejsu internetowego

Za pomocą przeglądarki należy wywołać interfejs użytkownika, aby skonfigurować przełącznik.
W menu **Basic Settings -> Network** (Ustawienia podstawowe -> Sieć) ustaw następujące wartości w zależności od wybranej topologii:
– Mode (Tryb): local (lokalny)
– Adres IP: wymagany adres IP, np. 192.168.1.201
– Ekran sieciowy: wymagany ekran sieciowy, np. 255.255.255.0
– Gateway: wymagana brama, np. 192.168.1.254 lub 0.0.0.0, jeśli brama nie jest wymagana
Kliknij przycisk **Write** (Zapisz).

Uwaga!
Ustawienia poszczególnych pozycji menu w konfiguracji przełącznika zostaną wprowadzone po kliknięciu przycisku **Write** (Zapisz).
Aby ustawienia zostały zapisane trwale, tzn. były przechowywane nawet po ponownym uruchomieniu urządzenia, należy w obszarze **Basic Settings -> Load/Save** (Ustawienia podstawowe -> Załaduj/Zapisz) w polu **Save** (Zapisz) zaznaczyć pole **On the device** (Na urządzeniu) i kliknąć przycisk **Save** (Zapisz).

10.3.2 Programowanie ustawień nadmiarowości

W sieciach central FPA wykorzystywany jest protokół RSTP jako protokół nadmiarowości, dlatego konieczne jest jego uaktywnianie i zaprogramowanie w interfejsie użytkownika konfiguracji:
W menu **Redundancy -> Spanning Tree -> Global** (Nadmiarowość -> Drzewo połączeń -> Globalne) ustaw następujące wartości:
– Function (Funkcja): On (Włączone)
– Protocol version (Wersja protokółu): RSTP

– Protocol configuration (Konfiguracja protokółu): użyj tych samych ustawień, jak w przypadku kontrolerów centrali

Kliknij przycisk **Write** (Zapisz).

Uwaga!
Ustawienia poszczególnych pozycji menu w konfiguracji przełącznika zostaną wprowadzone po kliknięciu przycisku **Write** (Zapisz).
Aby ustawienia zostały zapisane trwale, tzn. były przechowywane nawet po ponownym uruchomieniu urządzenia, należy w obszarze **Basic Settings -> Load/Save** (Ustawienia podstawowe -> Załaduj/Zapisz) w polu **Save** (Zapisz) zaznaczyć pole **On the device** (Na urządzeniu) i kliknąć przycisk **Save** (Zapisz).

10.3.3 Programowanie przekaźnika usterki

Uwaga!
Programowanie przekaźnika usterki jest wymagane tylko w przypadku zastosowań spełniających co najmniej jeden z poniższych warunków:
Istnieje połączenie pomiędzy dwoma przełącznikami. Jest to możliwe, np. w przypadku sieci szkieletowej z podpętlami.
Zasilanie przełącznika jest zaprojektowane nadmiarowo.

Uwaga!
Dokładny opis instalacji i konfiguracji przełączników można znaleźć w następujących dokumentach producenta:
Instrukcja instalacji
Skrócony przewodnik interfejsu internetowego

Za pomocą przeglądarki należy wywołać interfejs użytkownika, aby skonfigurować przełącznik.
W obszarze **Diagnosis -> Signal Contact** (Diagnostyka -> Styk sygnału) na karcie **Signal Contact 1** (Styk sygnału 1) ustaw w polu **Signal Contact Mode** (Tryb styku kontaktu) wartość **Device Status** (Stan urządzenia).
W obszarze **Diagnosis -> Device Status** (Diagnostyka -> Stan urządzenia) w polu **Monitoring** ustaw następujące wartości:
– **Power Supply 1** (Zasilacz 1): **Monitor** (Monitoruj)
– **Connection Error** (Błąd połączenia): **Monitor** (Monitoruj)
Dla wszystkich innych ustawień należy wybrać wartość **Ignore** (Ignoruj).

Uwaga!
Ustawienia pola **Device Status** (Stan urządzenia) dotyczą również wskaźnika LED usterki przełącznika.

Kliknij przycisk **Write** (Zapisz).

Uwaga!
Ustawienia poszczególnych pozycji menu w konfiguracji przełącznika zostaną wprowadzone po kliknięciu przycisku **Write** (Zapisz).
Aby ustawienia zostały zapisane trwale, tzn. były przechowywane nawet po ponownym uruchomieniu urządzenia, należy w obszarze **Basic Settings -> Load/Save** (Ustawienia podstawowe -> Załaduj/Zapisz) w polu **Save** (Zapisz) zaznaczyć pole **On the device** (Na urządzeniu) i kliknąć przycisk **Save** (Zapisz).

10.3.4 Programowanie monitoringu połączeń

Uwaga!
W przypadku używania przekaźnika usterki przełącznika jedynym potrzebnym ustawieniem jest monitoring połączeń.

Aby korzystać z przekaźnika usterki do monitorowania połączeń przełącznika, należy określić w konfiguracji przełącznika porty przełącznika, które mają być monitorowane.
Zaznacz pole wyboru **Forward Connection Error** (Przekaż błąd połączenia) dla poszczególnych portów w menu **Basic Settings -> Port Configuration** (Ustawienia podstawowe -> Konfiguracja portów).
Monitorowane będą tylko połączenia, dla których aktywowano opcję **Forward Connection Errors** (Przekaż błąd połączenia).
Kliknij przycisk **Write** (Zapisz).

Uwaga!
Ustawienia poszczególnych pozycji menu w konfiguracji przełącznika zostaną wprowadzone po kliknięciu przycisku **Write** (Zapisz).
Aby ustawienia zostały zapisane trwale, tzn. były przechowywane nawet po ponownym uruchomieniu urządzenia, należy w obszarze **Basic Settings -> Load/Save** (Ustawienia podstawowe -> Załaduj/Zapisz) w polu **Save** (Zapisz) zaznaczyć pole **On the device** (Na urządzeniu) i kliknąć przycisk **Save** (Zapisz).

10.3.5 Priorytet QoS, dotyczy tylko UGM-2040

W przypadku używania przełączników do wymiany danych pomiędzy sieciami FPA i UGM-2040 konieczne jest ustawienie priorytetu QoS w przełącznikach UGM.
W menu QoS/Priorität -> Global zmień ustawienia pola listy rozwijanej w obszarze Trusted Mode na wartość trustIpDscp.
Kliknij przycisk **Write** (Zapisz).

Uwaga!
Ustawienia poszczególnych pozycji menu w konfiguracji przełącznika zostaną wprowadzone po kliknięciu przycisku **Write** (Zapisz).
Aby ustawienia zostały zapisane trwale, tzn. były przechowywane nawet po ponownym uruchomieniu urządzenia, należy w obszarze **Basic Settings -> Load/Save** (Ustawienia podstawowe -> Załaduj/Zapisz) w polu **Save** (Zapisz) zaznaczyć pole **On the device** (Na urządzeniu) i kliknąć przycisk **Save** (Zapisz).

10.3.6 Jak włączyć śledzenie IGMP

Aby uniemożliwić przesyłanie ruchu multiemisji zgodnego z normą EN 54-2 do innych systemów połączonych z Ethernet Switch (Praesideo/PAVIRO, Remote Connect), należy aktywować śledzenie IGMP.
Na stronie konfiguracji IGMP dotyczącej Ethernet Switch wybierz następujące opcje:

1. Włącz śledzenie **IGMP**.
2. Aktywuj opcję **IGMP Querier** (Odpytywanie IGMP).
3. Skonfiguruj interwał transmisji, w którym RSR20 wysyła pakiety zapytań IGMP (np. 4 sekundy).
4. Skonfiguruj oczekiwany czas reakcji członków grup multiemisji na zapytania IGMP queries (np. 3 sekundy).
5. Wybierz opcję **Discard** (Odrzuć) dla pakietów z nieznanymi adresami multiemisji.

6. Wybierz opcję **Send to Query and registered Ports** (Wysyłaj do portów zapytania i zarejestrowanych) dla pakietów o znanych adresach multiemisji.
7. Włącz obsługę IGMP tylko dla portów, do których są podłączone inne systemy połączone z przełącznikiem. Wyłącz opcję **Static Query Port** (Statyczny port zapytania) dla wszystkich portów.

10.4 Sieć CAN

Połączenie z siecią i interfejsy

Kontroler centrali ma

– dwa interfejsy CAN (CAN1/CAN2) do połączeń z siecią (topologia odgałęzienia lub pętli)
– dwa wejścia sygnałowe (IN1/IN2)
– dwa interfejsy Ethernet
– Interfejs USB

W zależności od typu kontrolera centrali:

– dwa dodatkowe interfejsy Ethernet
– Interfejs RS232

Należy pamiętać, że długość kabla nie może przekraczać 3 m w przypadku podłączania do interfejsu USB lub 2 m w przypadku podłączania do interfejsu RS232.

Adresowanie i ustawienia w sieci

W zależności od typu kontrolera centrali:

– Adres węzła fizycznego jest konfigurowany w jej oprogramowaniu układowym podczas pierwszego uruchomienia.
– RSN na mechanicznych switchach obrotowych z tyłu centrali

Aby wyświetlić adres węzła fizycznego, jeśli jest zapisany w kontrolerze centrali:

▸ Wybierz **Konfiguracja** -> **Usługi sieciowe** -> **Ethernet** -> **Użyj ustaw. Ethernet** -> **Ustawienia IP** -> **Ustaw. domyślne**

Aby zmienić adres węzła fizycznego zapisany w kontrolerze centrali:

▸ Wyświetl ustawienia domyślne i zmień ostatni numer **adresu IP**.

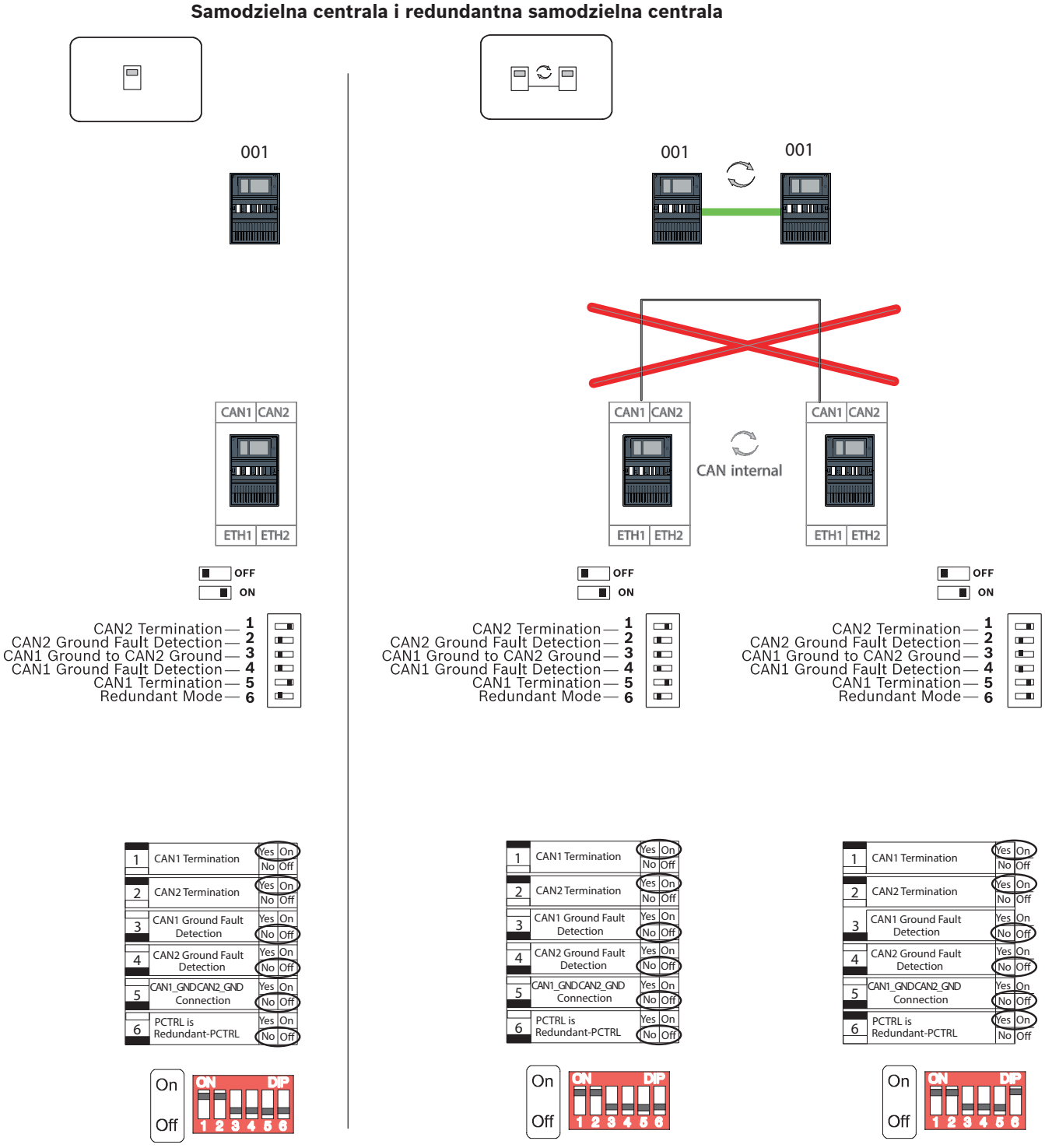
Aby zmienić mechaniczne RSN:

▸ Ustaw na mechanicznym switchu obrotowym z tyłu centrali wartość RSN i zanotuj ją na etykiecie poniżej tego switcha.

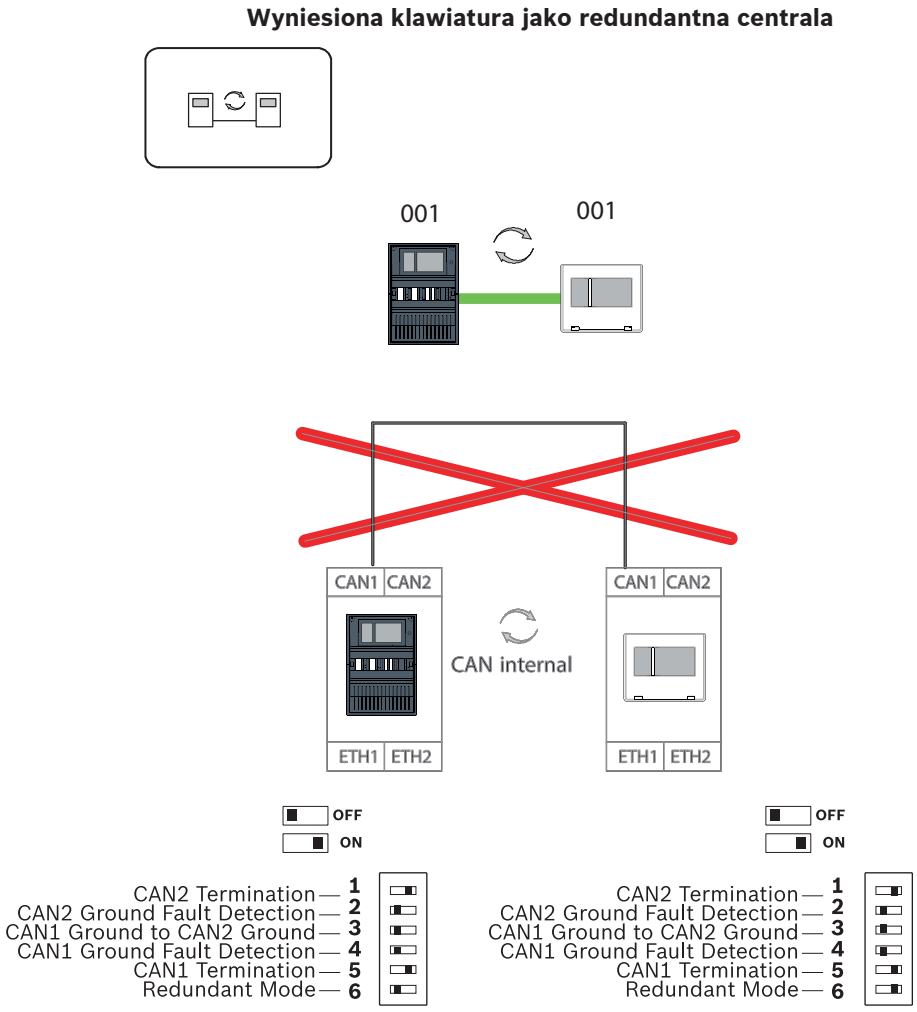
Konfiguracja topologii

Przełączniki DIP służące do ustawienia topologii są umieszczone z tyłu.

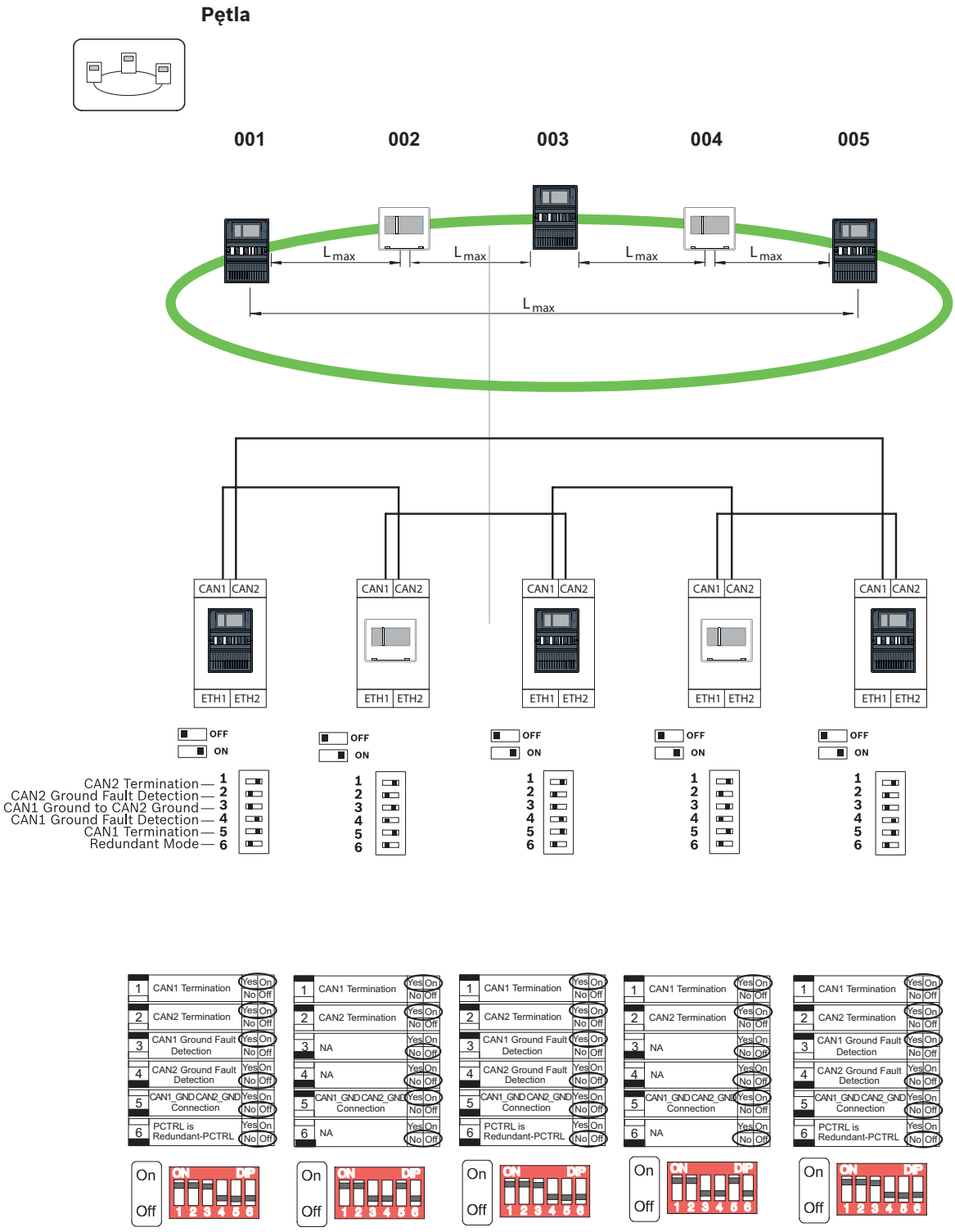
▸ Należy oznaczyć wybrane ustawienie na etykiecie w pobliżu przełączników DIP.



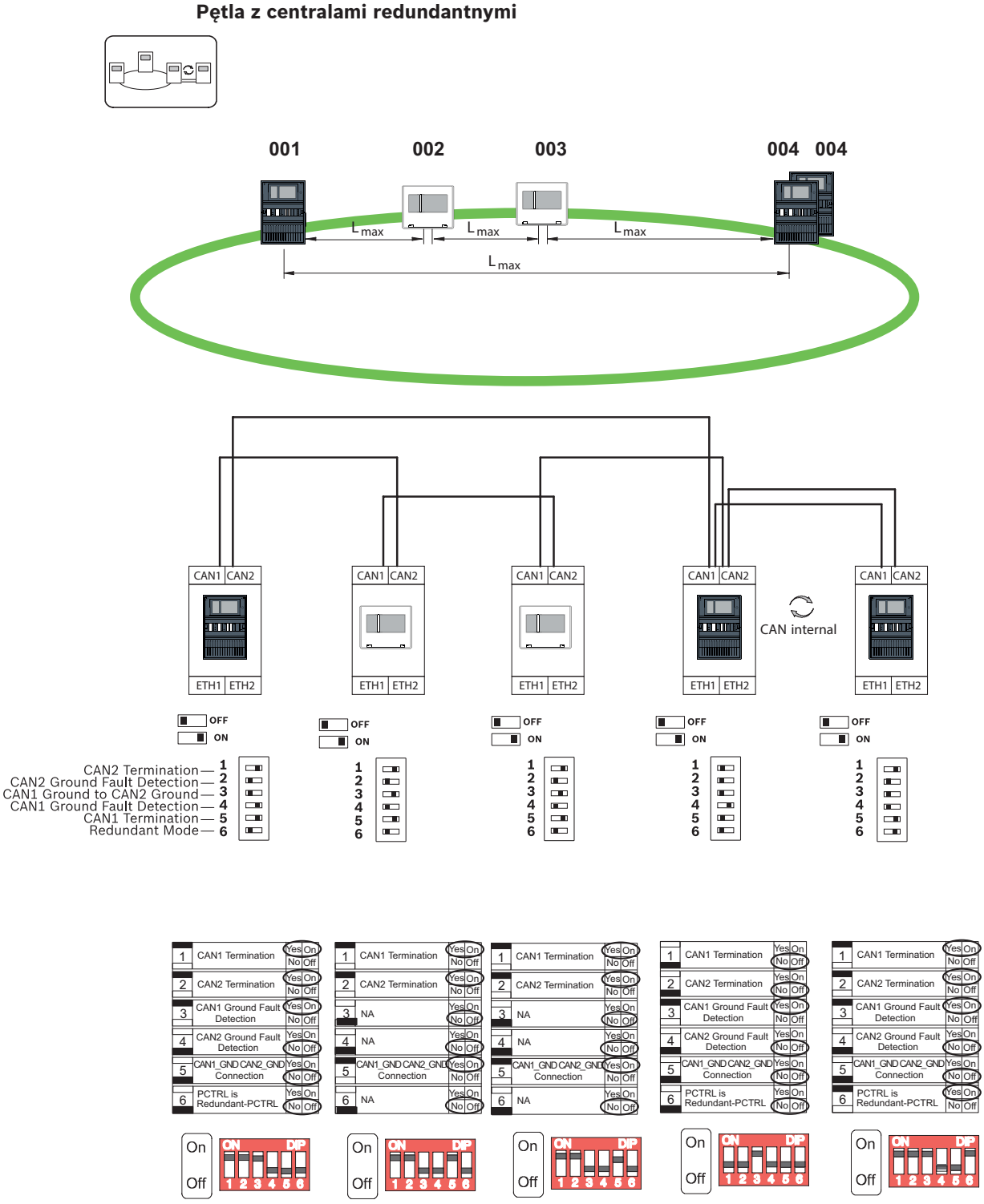
Rysunek 10.1: Ustawienia switcha DIP dla centrali autonomicznej (u góry: AVENAR, u dołu: FPA, po lewej: zwykła, po prawej: redundantna)



Rysunek 10.2: Ustawienia switcha DIP do konfiguracji klawiatury wyniesionej jako centrali redundantnej (tylko AVENAR)

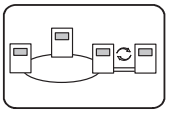


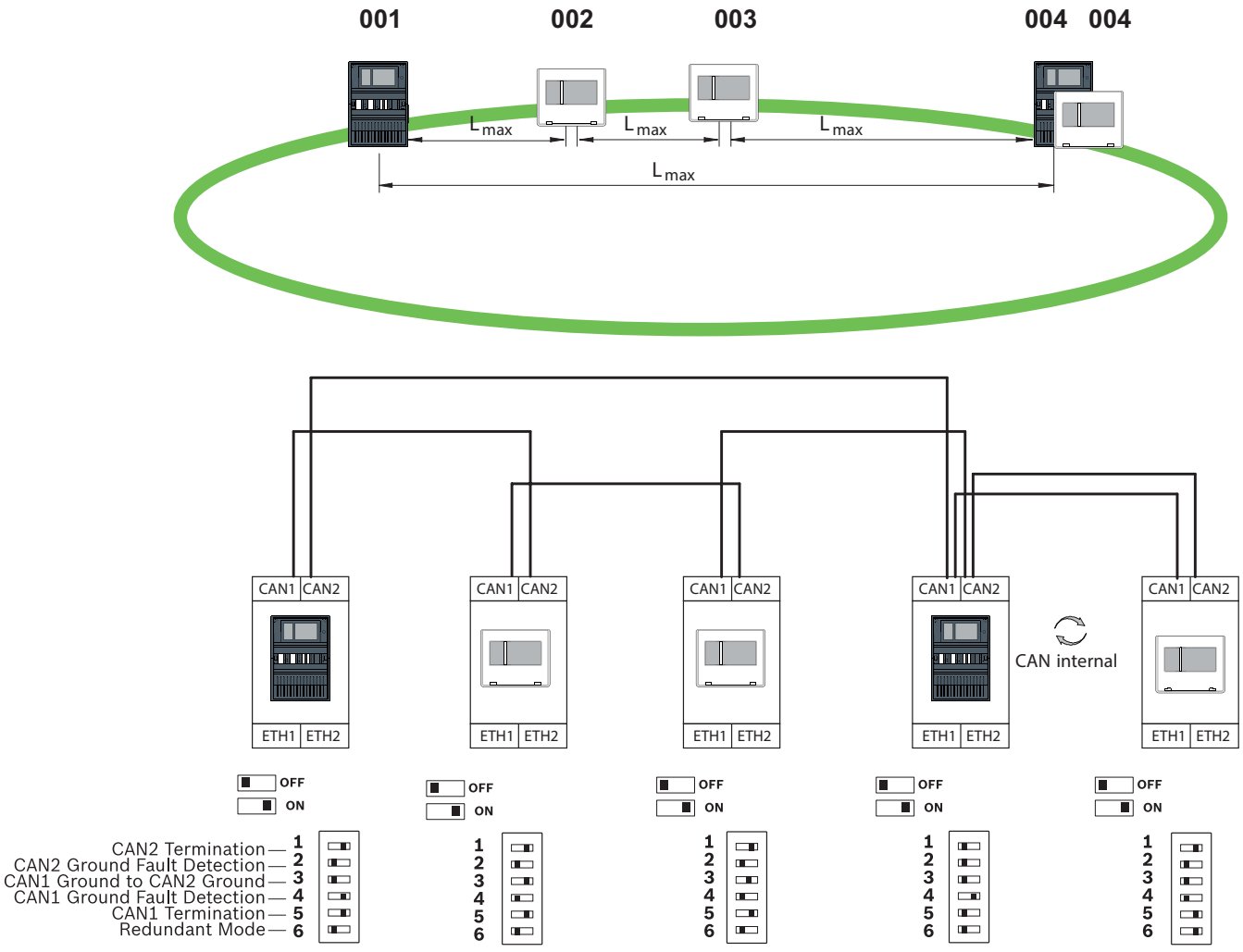
Rysunek 10.3: Ustawienia switcha DIP dla pętli (u góry: AVENAR, u dołu: FPA)



Rysunek 10.4: Ustawienia switcha DIP dla pętli z redundantnymi centralami (u góry: AVENAR, u dołu: FPA)

Pętla z klawiaturą wyniesioną jako centralą redundantną





Rysunek 10.5: Ustawienia switcha DIP do pętli z klawiaturą wyniesioną (tylko AVENAR)

11 Okablowanie

Aby utworzyć system zgodny z normą EN 54-2, przełączniki RSTP i konwertery transmisji muszą być podłączone za pośrednictwem monitorowanego zasilania centrali sygnalizacji pożaru.

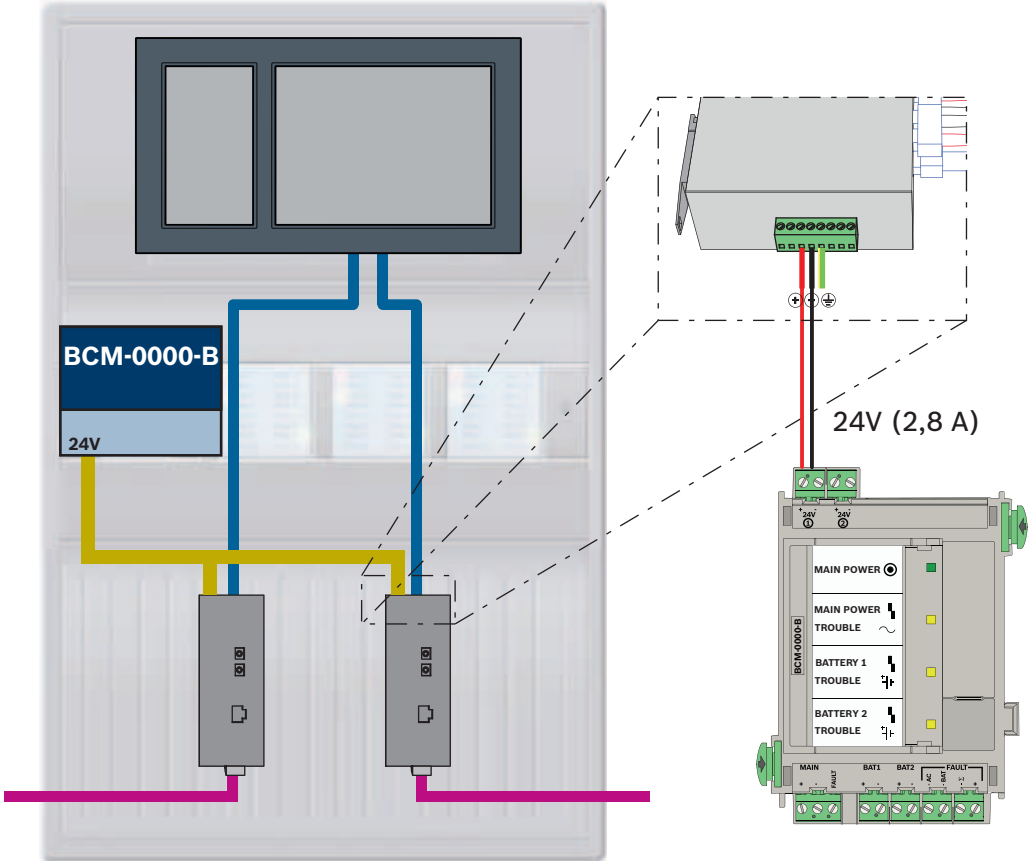
- Do zasilania konwerterów transmisji i przełączników RSTP należy używać wyjścia 24 V zasilacza BCM 0000 B lub FPP-5000.
- W przypadku podłączenia nadmiarowego zasilania lub utworzenia połączenia typu przełącznik-przełącznik wyjścia usterek przełącznika RSTP muszą być monitorowane za pośrednictwem wyjść centrali. Przykładem może być wykorzystanie wyjść kontrolera centrali lub IOP 0008 A.
- W przypadku konwertera transmisji należy aktywować funkcję LFP (Link Fault Pass-Through). Konfiguracja jest wykonywana przy użyciu przełącznika DIP konwertera transmisji.

Uwaga!
Instalacje sieciowe wymagają korzystania wyłącznie z następujących kabli:
Kabel Ethernet
Kabel sieciowy Ethernet, ekranowany, CAT5e lub lepszy.
Należy pamiętać o minimalnym promieniu zgięcia określonym w specyfikacji kabla.
Kabel światłowodowy
Tryb multi-mode: sieciowy kabel światłowodowy Ethernet, dupleks I-VH2G 50/125µ lub dupleks I-VH2G 62.5/125µ, wtyczka SC.
Tryb pojedynczy: sieciowy kabel światłowodowy Ethernet, dupleks I-VH2E 9/125µ, wtyczka SC.
Należy pamiętać o minimalnym promieniu zgięcia określonym w specyfikacji kabla.

11.1 Konwerter transmisji

Połączenie konwerterów transmisji

Uwaga!
Należy pamiętać o kierunku transmisji światłowodów FOC przy podłączaniu okablowania FX konwerterów transmisji.



Rysunek 11.1: Podłączenie konwertera transmisji do zasilania i kontrolera centrali IN1/IN2

Ikona	Opis
	Kabel TX Ethernet (miedziany)
	Kabel Ethernet FX (kabel światłowodowy)

Ikona	Opis
	Zasilanie 24 V
	Transmisja usterki
	Konwerter transmisji

11.2 Przełącznik Ethernet

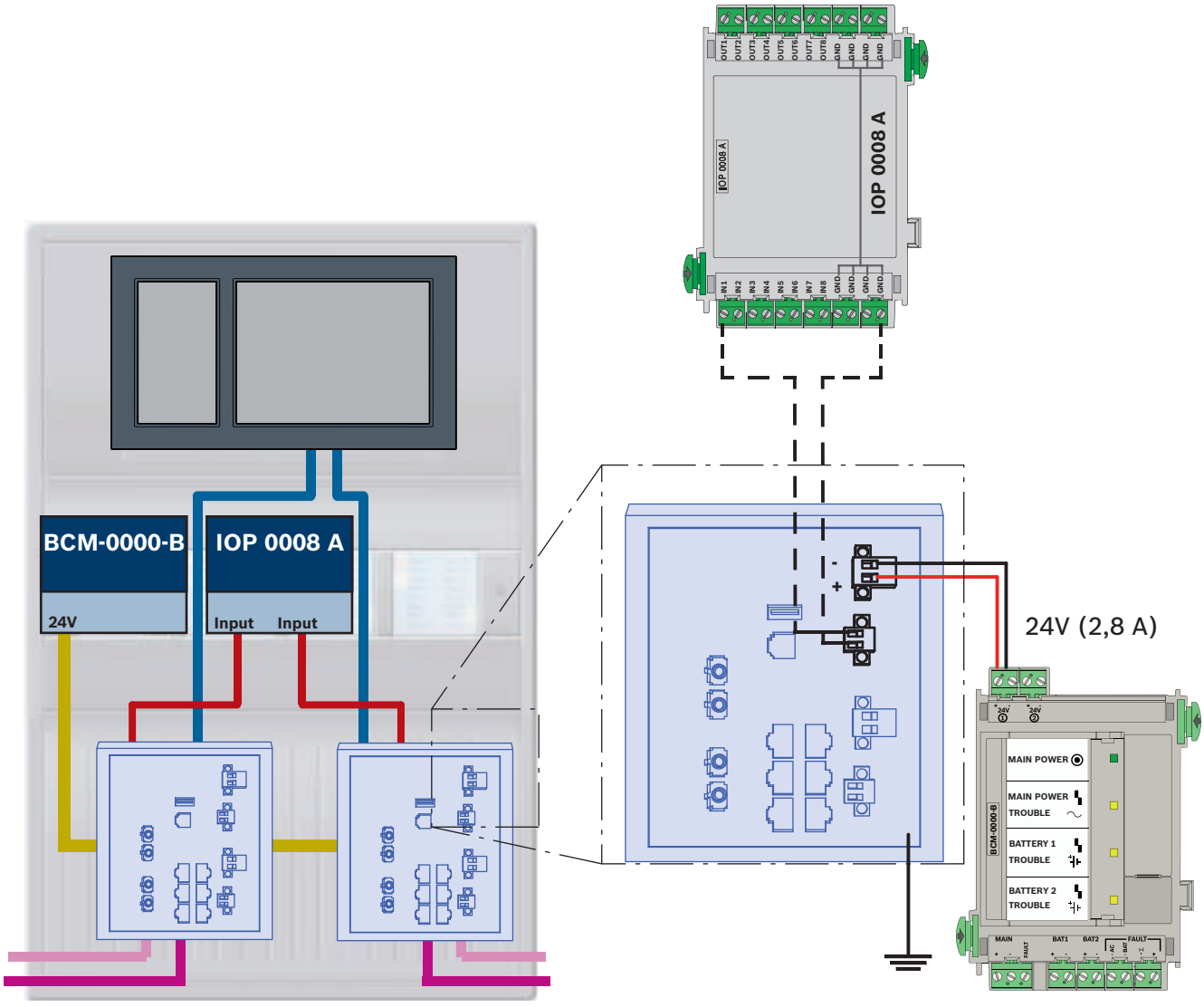
Połączenie switcha

Wyjścia sygnału usterki switchów można podłączyć do wejść kontrolera centrali lub modułu wejścia i wyjścia IOP.

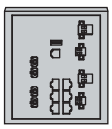
Uwaga!

Podłączenie przekaźnika usterki jest wymagane tylko w przypadku zastosowań spełniających co najmniej jeden z poniższych warunków:
Istnieje połączenie pomiędzy 2 switchami. Jest to możliwe, np. w przypadku sieci szkieletowej z podpętlami.
Zasilanie switcha jest zaprojektowane redundantnie.

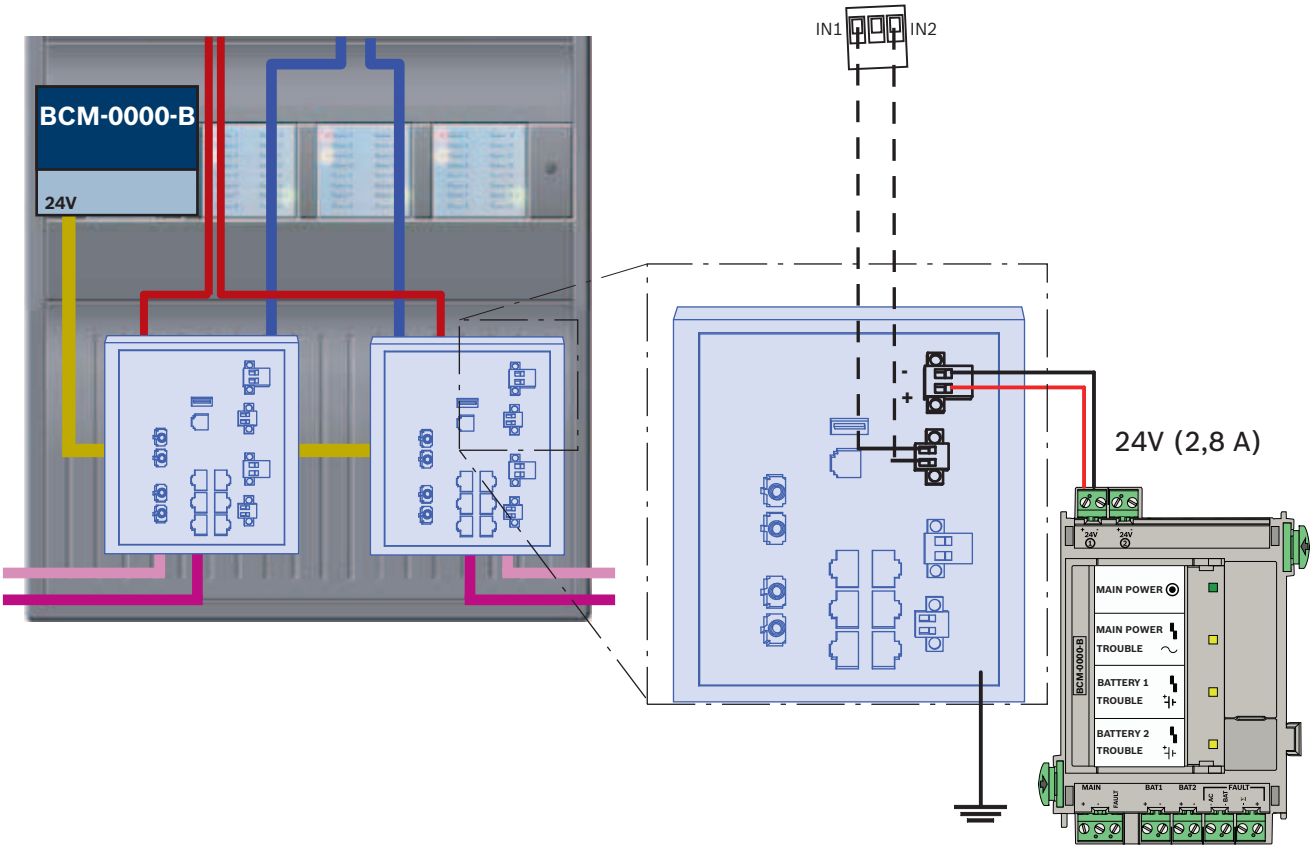
Podłączenie przełączników z raportowaniem usterek do wejść modułu IOP:



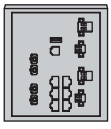
Rysunek 11.2: Podłączenie przełącznika do zasilania i modułu IOP

Ikona	Opis
	Kabel TX Ethernet (miedziany)
	Kabel Ethernet FX (kabel światłowodowy)
	Zasilanie 24 V
	Transmisja usterki
	Przełącznik RSTP

Podłączanie przełączników z raportowaniem usterek do wejść kontrolera centrali



Rysunek 11.3: Podłączenie przełącznika do zasilania i kontrolera centrali

Ikona	Opis
	Kabel TX Ethernet (miedziany)
	Kabel Ethernet FX (kabel światłowodowy)
	Zasilanie 24 V
	Transmisja usterki
	Przełącznik RSTP

Uwaga!
Przełączników nie należy podłączać za pomocą dostarczonego kabla sieciowego. Należy użyć kabla sieciowego Ethernet, ekranowanego, CAT5e lub lepszego.

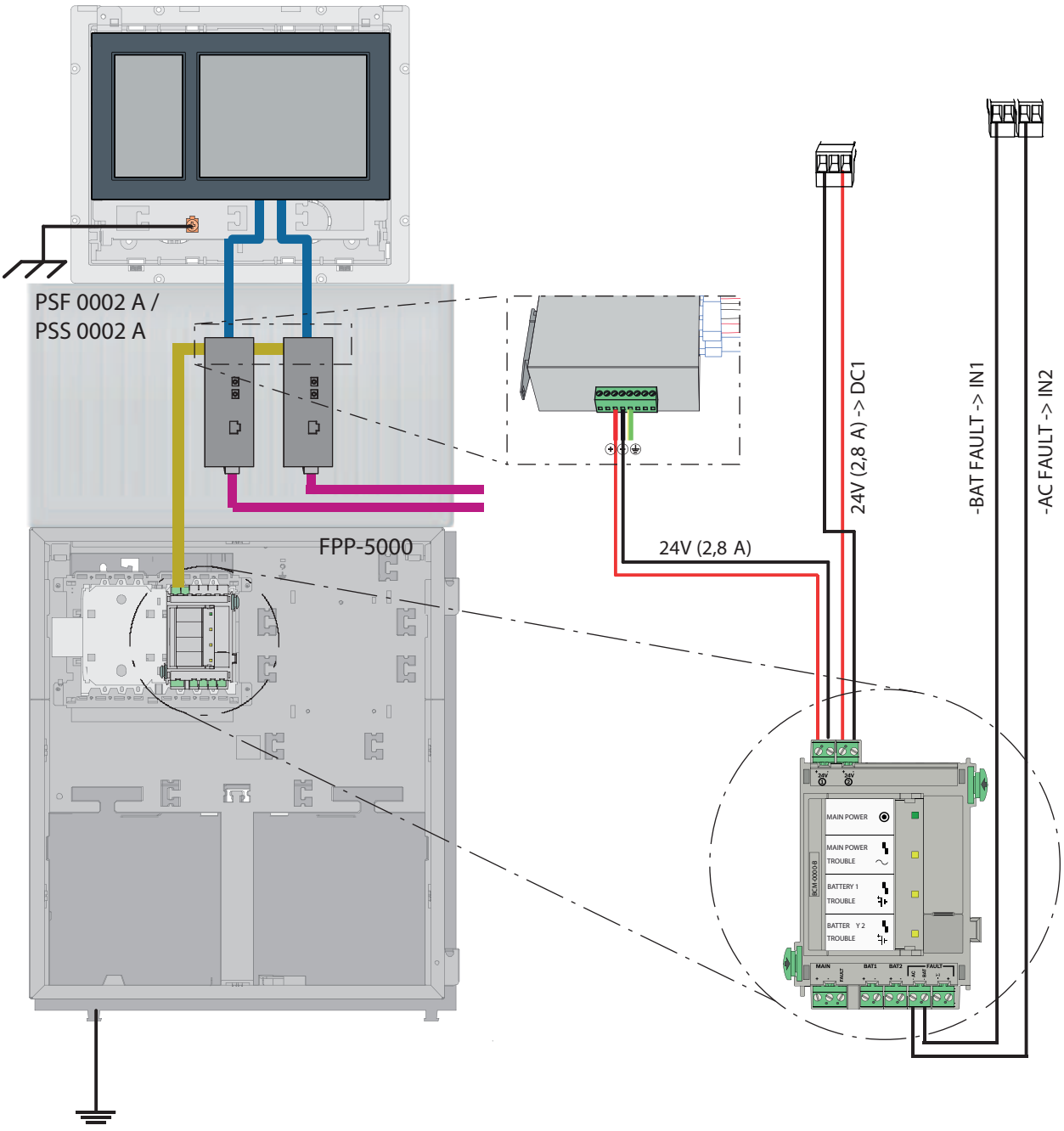
11.3 Zdalna klawiatura

Zdalna klawiatura musi być zasilana za pośrednictwem zewnętrznego zasilacza FPP-5000. Podłączenie do sieci jest tworzone przy użyciu dwóch konwerterów transmisji w PSS 0002 A lub USF 0000 A.

Uwaga!
Uwaga: zasilacz zewnętrzny FPP-5000 i PSF 0002 A (PSS 0002 A) muszą być zainstalowane w bezpośrednim sąsiedztwie (bez odstępu) zdalnej klawiatury. Dotknięcie kabli łączących między komponentami musi być niemożliwe, ponieważ kable nie są monitorowane pod kątem narastających zwarć i przerwań.

Uwaga!
Do podłączenia modułu zdalnej klawiatury do sieci central Ethernet należy używać wyłącznie konwerterów transmisji.
W przypadku zdalnej klawiatury niedozwolone jest użycie switchów.

Uwaga!
Zawsze podczas podłączania zdalnej klawiatury do sieci central Ethernet musi działać jej uziemienie.



Rysunek 11.4: Okablowanie zdalnej klawiatury

Ikona	Opis
	Kabel TX Ethernet (miedziany)
	Kabel Ethernet FX (kabel światłowodowy)
	Zasilanie 24 V
	Konwerter transmisji

12 Ustawienia FSP-5000-RPS

Aplikacja do programowania RPS umożliwia zaprogramowanie całej sieci za pośrednictwem portu USB, interfejsu sieciowego lub interfejsu szeregowego centrali. W tym celu należy skonfigurować ustawienia sieciowe w panelu, a następnie ponownie uruchomić centrale, aby uruchomić sieć.
Innym możliwym rozwiązaniem jest wykorzystanie interfejsu sieciowego przełącznika podłączonego do sieci.

12.1 Węzły sieci

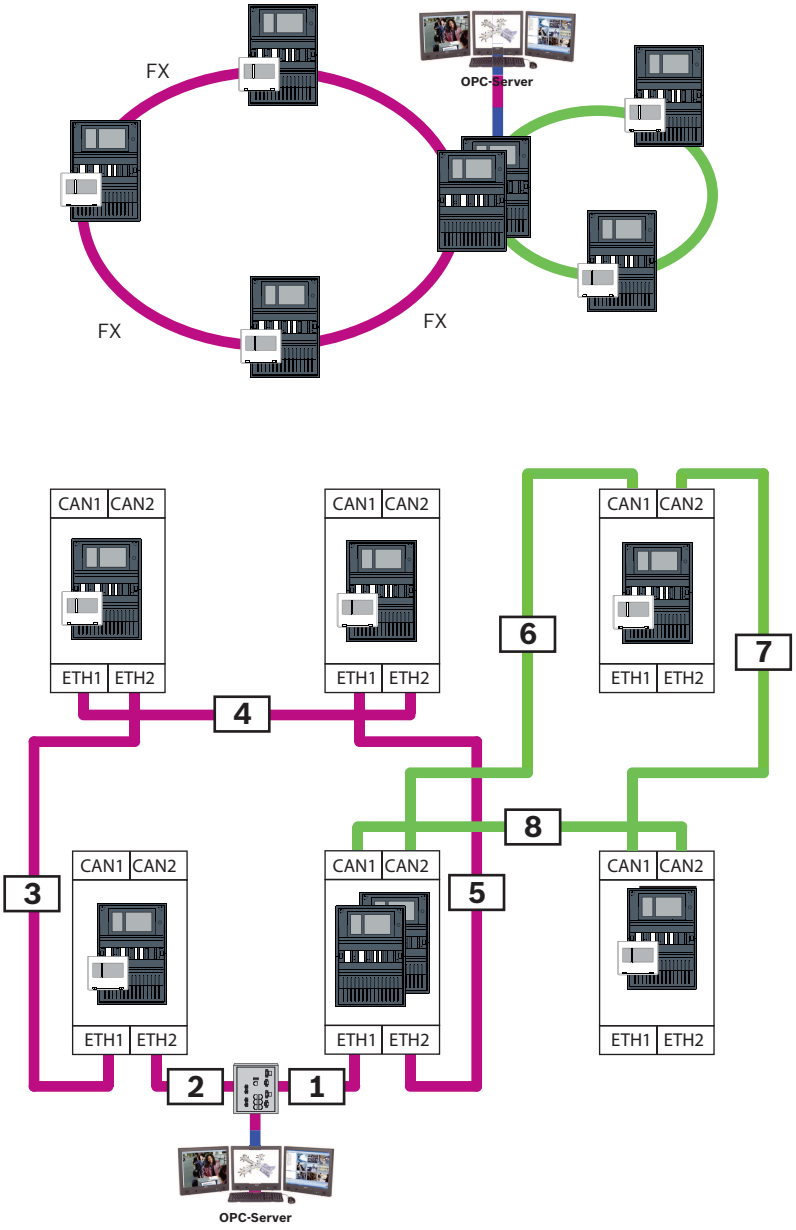
Należy zaprogramować całą sieć z wszystkimi węzłami sieci FSP-5000-RPS za pomocą aplikacji do programowania RPS, a następnie przesłać te dane do sieci. Aby to zrobić:

- Podłącz węzły FPA
  - Ustaw RSN w poszczególnych węzłach
- Dopasuj numery linii okablowania sieciowego, aby utworzyć planowaną topologię
- Sprawdź, czy wyświetlana topologia jest poprawna
- W razie potrzeby podłącz serwer OPC, system Praesideo/PAVIRO, serwer UGM-2040 i przełączniki
- Edytuj konfigurację adresu IP oraz sieci Ethernet
  - Przypisz adresy IP lub użyj standardowych ustawień, jeśli w topologii zastosowano mniej niż 20 węzłów RSTP
  - Wybierz odpowiedni protokół nadmiarowości dla ustawień topologii
- Wykonaj kontrolę spójności
- Podłącz się do sieci za pośrednictwem interfejsu Ethernet, USB lub szeregowego
- Wykonaj wielokrotne logowanie
- Wykonaj pełne automatyczne wykrywanie dla poszczególnych central
- Zażądaj informacji konfiguracyjnych i wykonaj wszystkie zadania

Po ponownym uruchomieniu sieci należy sprawdzić komunikaty o błędach i w razie potrzeby naprawić ewentualne błędy.

12.2 Numery linii

Należy przypisać numer linii do każdego używanego połączenia z siecią. Nie ma znaczenia, czy jest to połączenie CAN czy Ethernet.
Można użyć numeru jednej linii dla połączenia CAN i połączenia Ethernet. Aby jednak uzyskać lepszy obraz połączeń, można użyć różnych zakresów numerów.
Uwaga: jeśli używasz jako w oknie , wtedy numerem linii musi być 0 dla wszystkich połączeń.



Rysunek 12.1: Przykład sieci i możliwe numerowanie linii

12.3 Przełączniki

Jeśli w sieci używane są przełączniki, należy je utworzyć w aplikacji do programowania FSP-5000-RPS. Do każdego utworzonego przełącznika można przypisać maksymalnie 128 portów. Aby utworzyć sieć, do poszczególnych portów można przypisać numery podłączonych linii.

12.4 Serwery OPC

Serwery OPC w sieci muszą być dodane do aplikacji programującej FSP-5000-RPS.
W oprogramowaniu FSP-5000-RPS i na serwerze OPC muszą być skonfigurowane następujące ustawienia:

- Węzły sieci
- Grupa sieciowa
- RSN
- Adresy IP

– Port

Serwer OPC używa portu 25000 standardowo.

Uwaga!

EN 54

Połączenie systemu wizualizacji (np.BIS) za pośrednictwem interfejsu Ethernet przy użyciu serwera OPC lub serwera FSI jest zgodne z normą EN54, jeśli odpowiednie funkcje EN54 są wykonywane wyłącznie przez centralę sygnalizacji pożaru. Każda metoda kontroli lub administracji zgodna z normą EN54 (np. kontrola sygnalizatorów lub wyłączanie elementów) dostępna w systemie wizualizacji wymaga zastosowania certyfikowanego systemu integrującego.

Uwaga!

Aplikacja do programowania FSP-5000-RPS

Należy pamiętać o przypisaniu serwera OPC do każdego węzła sieci, z którego mają być przesyłane informacje o stanie.

12.5 Serwery UGM-2040

Uwaga!

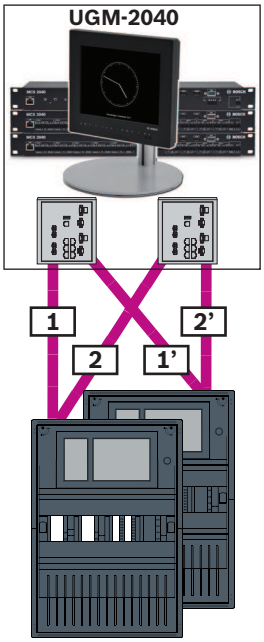
Wszystkie kontrolery centrali i serwery UGM muszą znajdować się w tej samej podsieci i mieć ten sam adres multicast.

W przypadku konfiguracji z wieloma centralami lub sieciami muszą one znajdować się w tej samej podsieci. Adresy multiemisji powinny się różnić.

Uwaga!

Należy pamiętać o przypisaniu serwera UGM-2040 do każdego węzła sieci, z którego mają być przesyłane informacje o stanie.

Aby podłączyć centralę do UGM-2040, należy symulować strukturę fizyczną sieci w oprogramowaniu RPS. Dotyczy to również numerów linii łączących kontroler centrali i przełączniki UGM-2040.



Rysunek 12.2: Przykład numerowania linii dla UGM-2040

13 Załącznik

13.1 Komunikaty o błędzie w sieci Ethernet

Należy pamiętać, że w każdym przypadku wystąpienia błędu wyświetlany jest komunikat o błędzie i błąd grupy.

Adres fizyczny	Adres logiczny	Komunikat o błędzie	Opis i możliwa przyczyna
Grupowanie usterek związanych z ogólną niesprawnością sieci			
135.0.1.0	Sieć 1.0		Niezgodna wersja oprogramowania sieciowego centrali. Istnieją 2 różne wersje oprogramowania.
Grupowanie usterek związanych z siecią			
135.0.6.1	Sieć 2.1		Ares IP został przypisany dwa razy.
135.0.6.2	Sieć 2.2		Konfiguracja IP raportującej centrali różni się od konfiguracji RPS.
135.0.6.3	Sieć 2.3		Konfiguracja redundancji (RSTP, parametr RSTP, system dwuadapterowy lub brak) centrali raportującej różni się od konfiguracji RPS.
Grupowanie usterek związanych z protokołem RSTP			
135.0.7.1	Sieć 3.1		Centrala raportująca przeszła z trybu RSTP do trybu STP (tryb zgodności). Urządzenie STP zostało podłączone do sieci.
135.0.7.2	Sieć 3.2		Topologia sieci RSTP została zmieniona. Na przykład dodano inne urządzenie RSTP do sieci. Komunikat ten może być generowany w przypadku przerwania linii.

Adres fizyczny	Adres logiczny	Komunikat o błędzie	Opis i możliwa przyczyna
135.0.7.3	Sieć 3.3		Stanem portu RSTP centrali raportującej nie jest punkt-punkt. Na przykład, gdy kilka urządzeń RSTP zostało podłączonych do portu RSTP. Albo gdy inne urządzenie RSTP podłączono do portu RSTP za pośrednictwem linii półdupleksowej.
Grupowanie usterek związanych z połączeniem sieciowym			
135.0.5.1	Połączenie sieciowe 1.0		Transmisja danych do magistrali CAN 1 jest ograniczona. Możliwe przyczyny to m.in. uszkodzenia kabli, rozłączone kable, zakłócenia kablowe.
135.0.5.2	Połączenie sieciowe 2.0		Transmisja danych do magistrali CAN 2 jest ograniczona. Możliwe przyczyny to m.in. uszkodzenia kabli, rozłączone kable, zakłócenia kablowe.
135.0.5.3	Połączenie sieciowe 3.0		Transmisja danych do linii Ethernet 1 jest ograniczona. Możliwe przyczyny to m.in. uszkodzenia kabli, rozłączone kable, zakłócenia kablowe.
135.0.5.4	Połączenie sieciowe 4.0		Transmisja danych do linii Ethernet 2 jest ograniczona. Możliwe przyczyny to m.in. uszkodzenia kabli, rozłączone kable, zakłócenia kablowe.

Indeks

Symbole

A

B

D

E

I

K

L

M

P

R

S

T

U

Bosch Sicherheitssysteme GmbH
Robert-Bosch-Ring 5
85630 Grasbrunn
Germany
www.boschsecurity.com
© Bosch Sicherheitssysteme GmbH, 2020