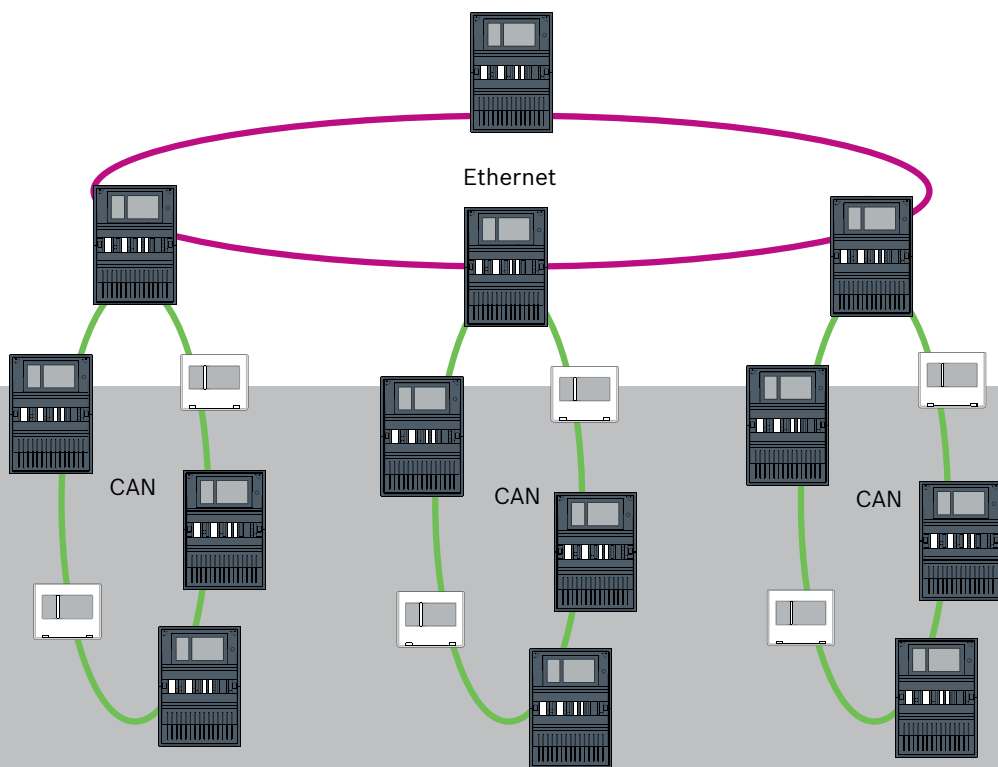


AVENAR panel | FPA-5000 | FPA-1200



Spis treści

1	Bezpieczeństwo	5
1.1	Środki organizacyjne na komputerze PC dotyczące uruchamiania klientów usługi	5
1.2	Objaśnienie symboli bezpieczeństwa	6
1.3	Ostrzeżenia dotyczące bezpieczeństwa	6
2	Wstęp	8
3	Ogólne informacje o systemie	9
4	Topologie	11
4.1	Pętla CAN	16
4.2	Pętla Ethernet	16
4.3	Podwójna pętla Ethernet/CAN	16
4.4	Pętla CAN z segmentami sieci Ethernet	17
4.5	Sieć szkieletowa Ethernet z podpętlami (Ethernet/CAN)	17
4.6	Podłączanie pętli Ethernet	18
5	Sieć Ethernet	19
5.1	Protokoły	20
5.2	Średnica sieci	20
5.3	Stosowane kable	23
5.4	Tworzenie lub modyfikowanie sieci Ethernet	23
6	Sieć CAN	25
6.1	Tworzenie lub modyfikowanie sieci CAN	26
7	Schemat sieci Ethernet i CAN	26
7.1	Łączenie central w sieć Ethernet	28
7.2	Łączenie central w sieć CAN	29
7.3	Podłączanie usług do centrali	29
7.4	Sieć central w sieci Ethernet z centralami redundantnymi	30
7.5	Sieć central w sieci CAN z centralami redundantnymi	31
7.6	Połączenie centrali z siecią za pomocą dwóch pętli sieci Ethernet	31
7.7	Sieć central w dwóch pętlach sieci Ethernet z centralami redundantnymi	32
7.8	Połączenia sieci Ethernet i CAN z centralami redundantnymi	32
7.9	Podłączanie usług zdalnych do central redundantnymi	32
7.9.1	Nadmiarowa centrala AVENAR panel	33
7.9.2	Redundantny FPA	34
7.10	Podłączanie usług ratowania życia do central nadmiarowych	34
8	Usługi Remote Services	35
8.1	Warunki wstępne korzystania ze zdalnych usług Remote Services	35
8.1.1	Remote Connect	35
8.1.2	Eksplorator systemu przeciwpożarowego	38
8.2	Remote Alert	39
8.3	Usługa Remote Maintenance	39
8.4	Usługa Remote Maintenance dla sieci Private Secure Network	40
9	System zarządzania budynkiem	41
10	Inteligentne łącze bezpieczeństwa	44
10.1	Jeden bezpośredni interfejs do systemu VAS	45
10.1.1	Praesideo i PAVIRO	45
10.1.2	PRAESENSA	46
10.2	Wiele bezpośrednich interfejsów do systemu VAS	47
10.3	System VAS zintegrowany w sieci central połączonych przez Ethernet	48
11	System integrujący	49

12	Instalacja	50
12.1	Ustawienia konwertera transmisji	50
12.2	Montaż przełącznika Ethernet	52
12.3	Ustawienia przełącznika	52
12.3.1	Przypisanie adresu IP	52
12.3.2	Programowanie ustawień nadmiarowości	53
12.3.3	Programowanie przekaźnika usterki	54
12.3.4	Programowanie monitoringu połączeń	54
12.3.5	Priorytet QoS	55
12.3.6	Jak włączyć śledzenie IGMP	55
12.4	Sieć CAN	56
13	Okablowanie Ethernet	61
13.1	Konwerter transmisji	62
13.2	Przełącznik Ethernet	63
13.3	Zdalna klawiatura	66
14	Ustawienia FSP-5000-RPS	68
14.1	Węzły sieci	68
14.2	Numery linii	68
14.3	Przełączniki	69
15	Załącznik	69
15.1	Komunikaty o błędzie w sieci Ethernet	69
	Indeks	71

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 posortowane 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.



Przeestroga!

Ostrzeżenie informuje o ryzyku uszkodzenia przedmiotów.



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



Przeestroga!

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

**Przeestroga!**

Usługi Remote Services wymagają bezpiecznego połączenia IP. Wymagane jest połączenie z Bosch Remote 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.

**Przeestroga!**

Konfiguracja ustawień sieciowych centrali sygnalizacji pożarowej wymaga osobnej sieci Ethernet.

Stosowanie systemu sygnalizacji pożaru w jakiegokolwiek innej sieci Ethernet jest możliwe na własne ryzyko użytkownika. Firma Bosch nie ponosi żadnej odpowiedzialności za skutki niewłaściwego użycia.

W przypadku użycia niewyłączonej sieci Ethernet nie można zapewnić w pełni niezawodnej transmisji alarmu i bezpieczeństwa sieci IT.

Inteligentne łącze bezpieczeństwa**Ostrzeżenie!**

Zagrożenia dla bezpieczeństwa podczas korzystania z sieci Ethernet

Nie łączyc urządzeń systemu PRAESENSA z centralami FPA-5000/FPA-1200 za pośrednictwem funkcji Smart Safety Link ze względu na zagrożenia dla bezpieczeństwa powodowane przez sieć Ethernet.

**Uwaga!**

VdS 2540

Dźwiękowy system alarmowy musi być zamontowany w jednej płaszczyźnie z centralą sygnalizacji pożaru w tym samym pomieszczeniu. W przeciwnym razie nie zostaną spełnione wymagania dyrektywy VdS 2540 dla torów transmisji danych.

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 między węzłami musi być mniejsza niż 100 m.

**Uwaga!**

VdS 2540 – Sieć Ethernet

Jeśli chodzi o centrale łączone w sieci Ethernet, należy pamiętać, że w przypadku instalacji w Niemczech, gdzie wymagana jest zgodność z normą VdS 2540, do wszystkich ścieżek transmisji danych musi być używany kabel światłowodowy. Jedynym wyjątkiem jest tu wnętrze obudowy.

**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.

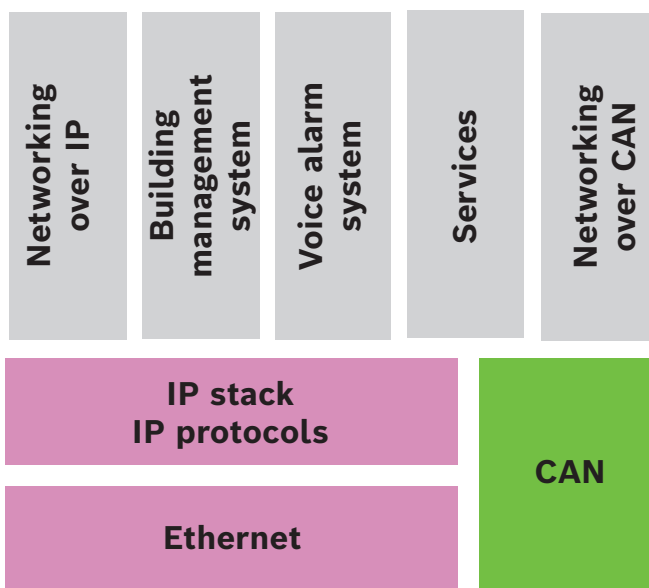
Szczegółowe opisy instalowania poszczególnych elementów można znaleźć w odpowiednich instrukcjach instalacji.

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 poprzez TCP/IP. Wyłączenie interfejsu może być konieczne dla połączenia poprzez CAN.

Włączanie usług

- Połączenie sieciowe za pośrednictwem TCP/IP
W FSP-5000-RPS włącz komunikację między centralami w sieci Ethernet
- System zarządzania budynkiem
Utwórz serwer w konfiguracji FSP-5000-RPS
- Połączenie z dźwiękowym systemem alarmowym
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!


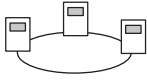

Niezamierzony transfer danych


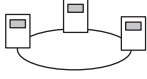

Jeśli interfejs Ethernet kontrolera centrali ma służyć jedynie do komunikacji z systemem zarządzania budynkiem lub Remote Services, wyłącz połączenie centrali z siecią poprzez TCP/IP w FSP-5000-RPS. W przeciwnym razie dane pożarowe mogą być przesyłane przez sieć Ethernet w niezamierzony sposób.

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. 32 panele/ 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
 Redundancja central	Możliwe	Brak możliwości (mikroswitch DIP 6 kontrolera centrali nie działa).

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!**

Wersje oprogramowania sprzętowego

W systemie zawierającym wyłącznie węzły AVENAR zaleca się używanie najnowszego oprogramowania układowego central o numeracji wersji 4.x.

W systemie zawierającym co najmniej jeden węzeł FPA/FMR zaleca się używanie najnowszego oprogramowania układowego central o numeracji wersji 3.x.

**Uwaga!**

Od 1 stycznia 2022 r. do 31 grudnia 2025 r. oprogramowanie sprzętowe central w wersji 3.x jest w trybie konserwacji. W tym okresie zostaną wydane nowe wersje zawierające poprawki krytycznych błędów i krytycznych luk w zabezpieczeniach. Nie planuje się dodawania żadnych nowych funkcji, urządzeń peryferyjnych LSN, języków graficznego interfejsu użytkownika i zmian normatywnych.

Po 31 grudnia 2025 r. uruchamianie oprogramowania układowego w wersji 3.x na centralach podłączonych do interfejsu Ethernet lub sieci zwiększa ryzyko dla bezpieczeństwa. Zdecydowanie zaleca się przeprowadzenie oceny ryzyka bezpieczeństwa.

Po zidentyfikowaniu zagrożeń bezpieczeństwa obowiązkowe jest uaktualnienie centrali AVENAR paneli uruchomienie najnowszej wersji oprogramowania układowego do wersji 4.x.

**Uwaga!**

Redundantny kontroler centrali

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

4

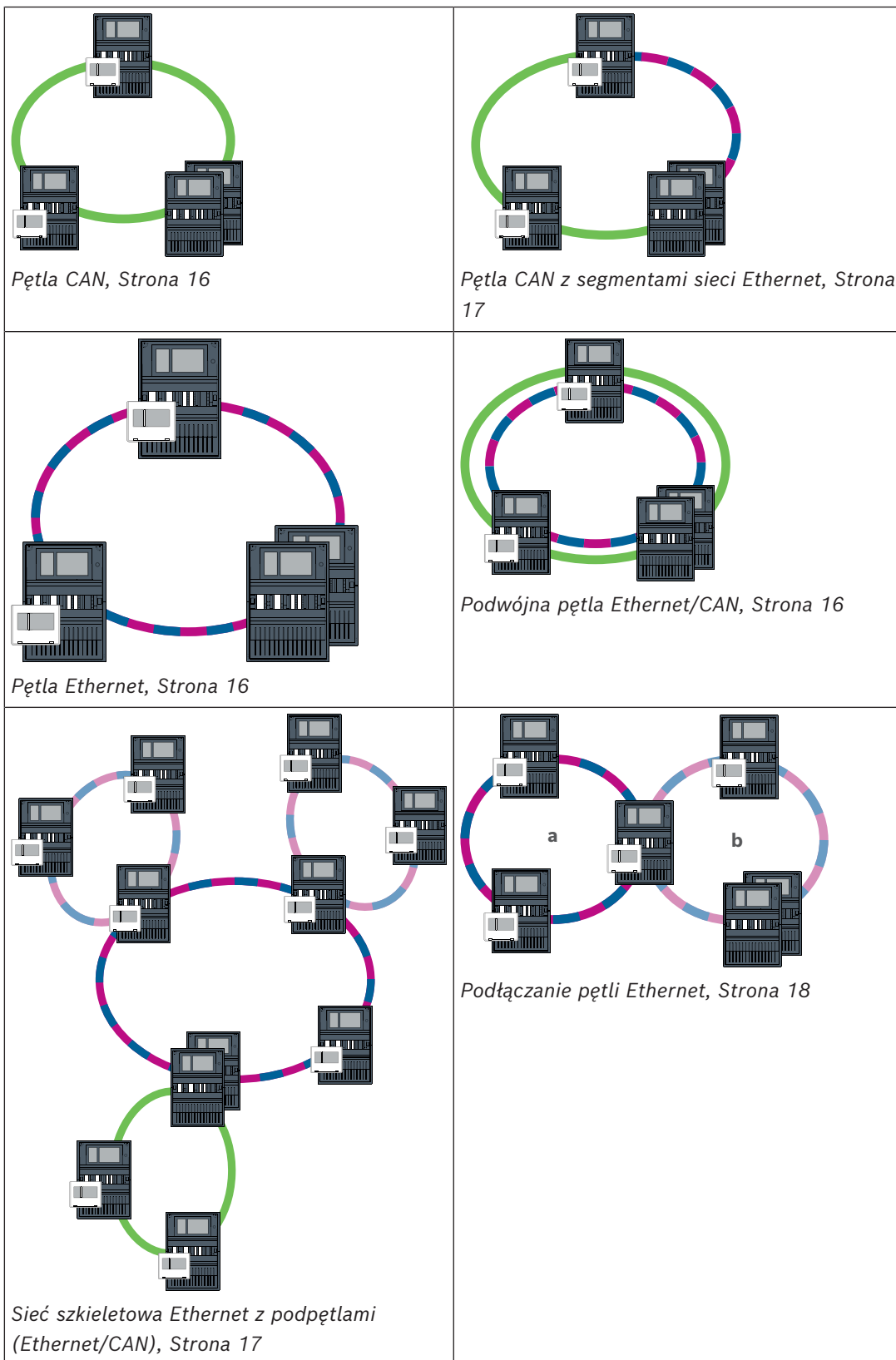
Topologie

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




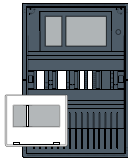
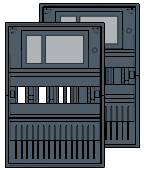
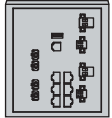



**Uwaga!**

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.



Kabel	Opis
	Kabel Ethernet TX (miedziany), długość kabla TX pomiędzy węzłami < 100 m

Kabel	Opis
	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)
	Centrala standardowa lub nadmiarowa (w topologii sieci Ethernet wewnętrzny przełącznik RSTP) Klawiatura wyniesiona może być używana jako redundanthy kontroler centrali. Połączenia sieciowe i ustawienia są identyczne dla redundanтного kontrolera centrali i redundanтnej klawiatury. Używanie redundanтnej 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
	System zarządzania budynkiem

Ograniczenia w sieci

Sieć zawiera węzły.

- Węzeł to kontroler centrali, zdalna klawiatura lub serwer (serwer BACnet, serwer FSI, serwer OPC lub serwer UGM).
- Maksymalna liczba węzłów to 32
- Maksymalna liczba punktów logicznych na sieć wynosi 32768.
- Liczba punktów logicznych na centralę działającą w sieci jest ograniczona do 2048.
- Liczba zdalnych klawiatur, które można przypisać do jednej centrali, jest ograniczona do 3.
- Liczba serwerów, które można przypisać do jednej centrali lub zdalnej klawiatury, jest ograniczona do:
 - 1 BACnet server
 - 2 FSI server
 - 1 OPC server
 - 2 UGM server

Więcej informacji można znaleźć w części poświęconej limitom systemu w instrukcji obsługi systemu.

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, zdalna klawiatura lub serwer 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 switchy 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 alarmowych. W przypadku przekroczenia tej liczby centrala musi być zaprojektowana redundantnie.
Jeśli centrala działa jako interfejs z podpętlą CAN i więcej niż 512 punktami alarmowymi w podpętli, to należy ją również zaprojektować z uwzględnieniem nadmiarowości. Przetłącznik RSTP, który łączy 2 pętle, zapewnia redundancję.



Uwaga!

Liczba punktów logicznych
W przypadku centrali samodzielnej można podłączyć 4096 punktów logicznych, nawet jeśli została ona zaprojektowana jako redundantna. Jeśli centrala znajduje się w sieci, można podłączyć maksymalnie 2048 punktów logicznych.



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 multimijsji 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 switchy zewnętrzne RSTP są traktowane jako switchy RSTP. Nadmiarowe kontrolery centrali nie są traktowane jak switchy 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

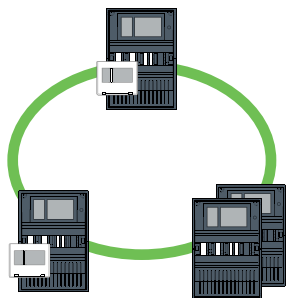
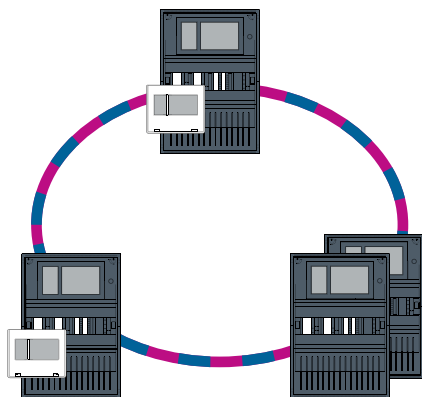
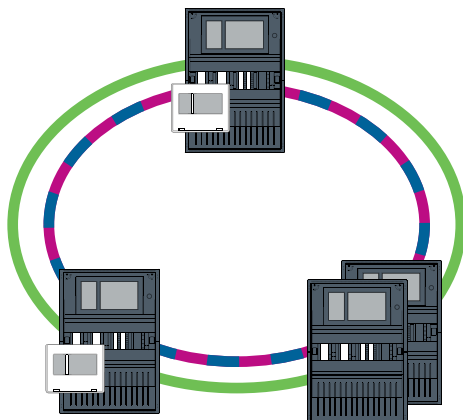
Parametry

- W pętli można wykorzystać maksymalnie 32 węzły.
- Średnica sieci nie może być większa niż 32, patrz *Średnica sieci*, Strona 20.

- Przetaczniki Ethernet nie mogą być używane na zewnątrz obudów central.
- Konwertery transmisji nie mogą być używane na zewnątrz obudów central.

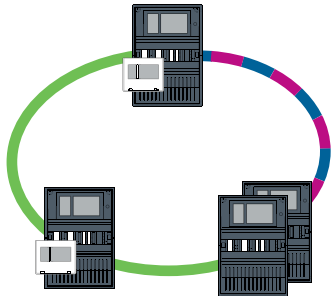
Funkcje

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

4.1**Pętla CAN****Rysunek 4.1:** Pętla CAN**4.2****Pętla Ethernet****Rysunek 4.2:** Pętla Ethernet**4.3****Podwójna pętla Ethernet/CAN****Rysunek 4.3:** Podwójna pętla Ethernet i CAN

4.4 Pętla CAN z segmentami sieci Ethernet

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



Rysunek 4.4: Pętla CAN z segmentami sieci Ethernet

4.5 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 15.



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 alarmowych.

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!

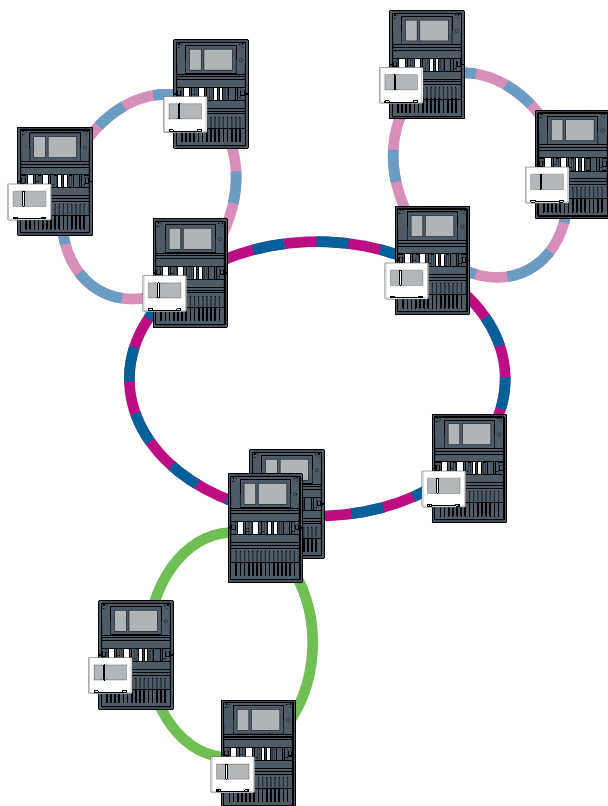
Dla wszystkich przełączników RSTP w sieci szkieletowej należy ustawić priorytet RSTP wyższy niż w podpętlach. Dzięki temu most główny RSTP zawsze pozostanie w sieci szkieletowej, nawet w przypadku usterki.

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.



Rysunek 4.5: Sieć szkieletowa Ethernet z podpętlami

4.6

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!**

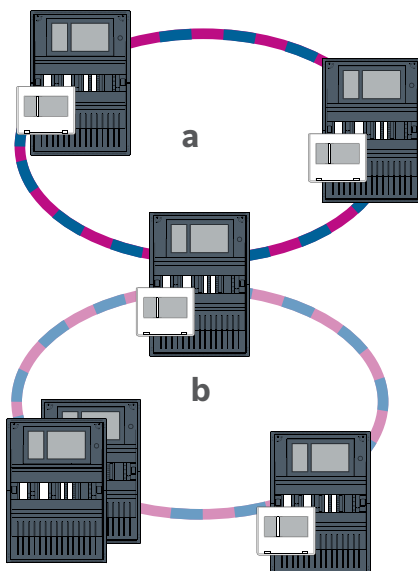
Dla wszystkich central i przełączników w sieci szkieletowej należy ustawić priorytet RSTP wyższy niż w podpętlach. Dzięki temu most główny RSTP zawsze pozostanie w sieci szkieletowej, nawet w przypadku usterki.

Przełączniki podłączające dwie pętle są częścią sieci szkieletowej!

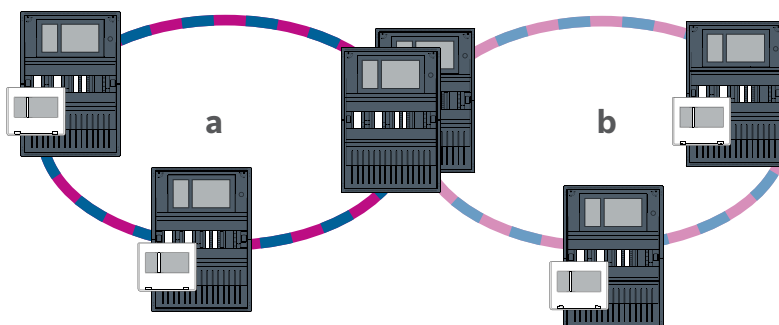
W sieci szkieletowej należy używać priorytetu RSTP 16384.

**Uwaga!**

Im niższa jest wartość ustawienia, tym wyższy priorytet RSTP.



Rysunek 4.6: Podłączenie pętli Ethernet za pośrednictwem centrali nienadmiarowej



Rysunek 4.7: Podłączenie 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 podłączenia systemu zarządzania budynkiem, dźwiękowego systemu alarmowego lub systemu integrującego 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, ETH4 można wykorzystać do podłączenia systemu zarządzania budynkiem, dźwiękowego systemu alarmowego lub systemu integrującego.
4. Jeśli centrala nie jest połączona z siecią przez ETH1 i ETH2, każdy z nich może być użyty do podłączenia systemu zarządzania budynkiem, dźwiękowego systemu alarmowego lub systemu integrującego.

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



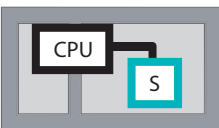
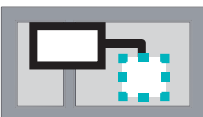
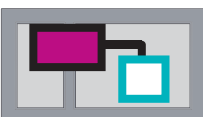
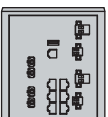
Średnica sieci odpowiada liczbie przełączników RSTP na najdłuższym możliwym odcinku bez pętli pomiędzy dowolnymi dwoma końcowymi punktami sieci.

Należy wziąć pod uwagę następujące kwestie dotyczące sieci RSTP Ethernet central:

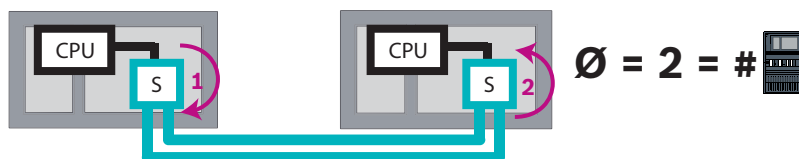
- Każdy kontroler centrali zawiera punkt końcowy i wewnętrzny przełącznik RSTP.

- 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.
- Systemy zarządzania budynkiem nie są brane pod uwagę w odniesieniu do średnicy.

Klucz

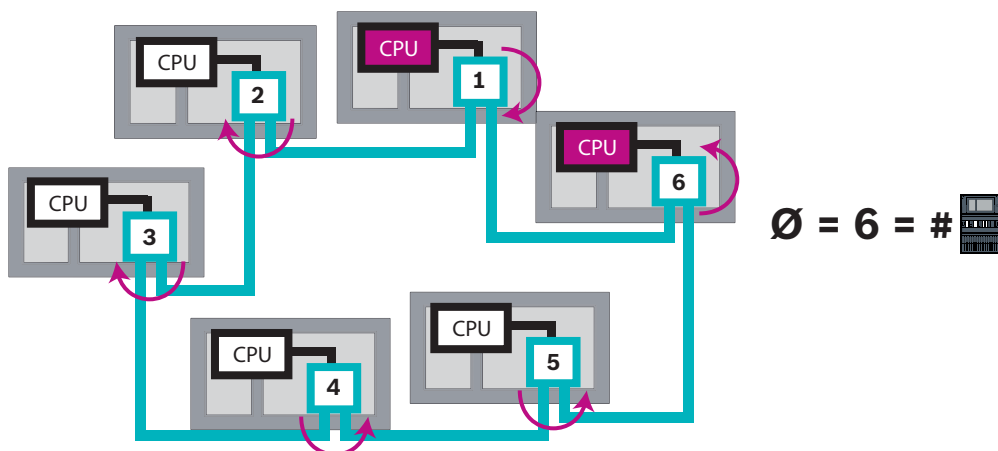
	Procesor główny w kontrolerze centrali lub w zdalnej klawiaturze.
	Wewnętrzny przełącznik RSTP w kontrolerze centrali lub w zdalnej klawiaturze.
	Kontroler centrali lub zdalna klawiatura z procesorem głównym i wewnętrznym przełącznikiem RSTP.
	Nadmiarowy kontroler centrali z procesorem głównym i wewnętrznym 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.

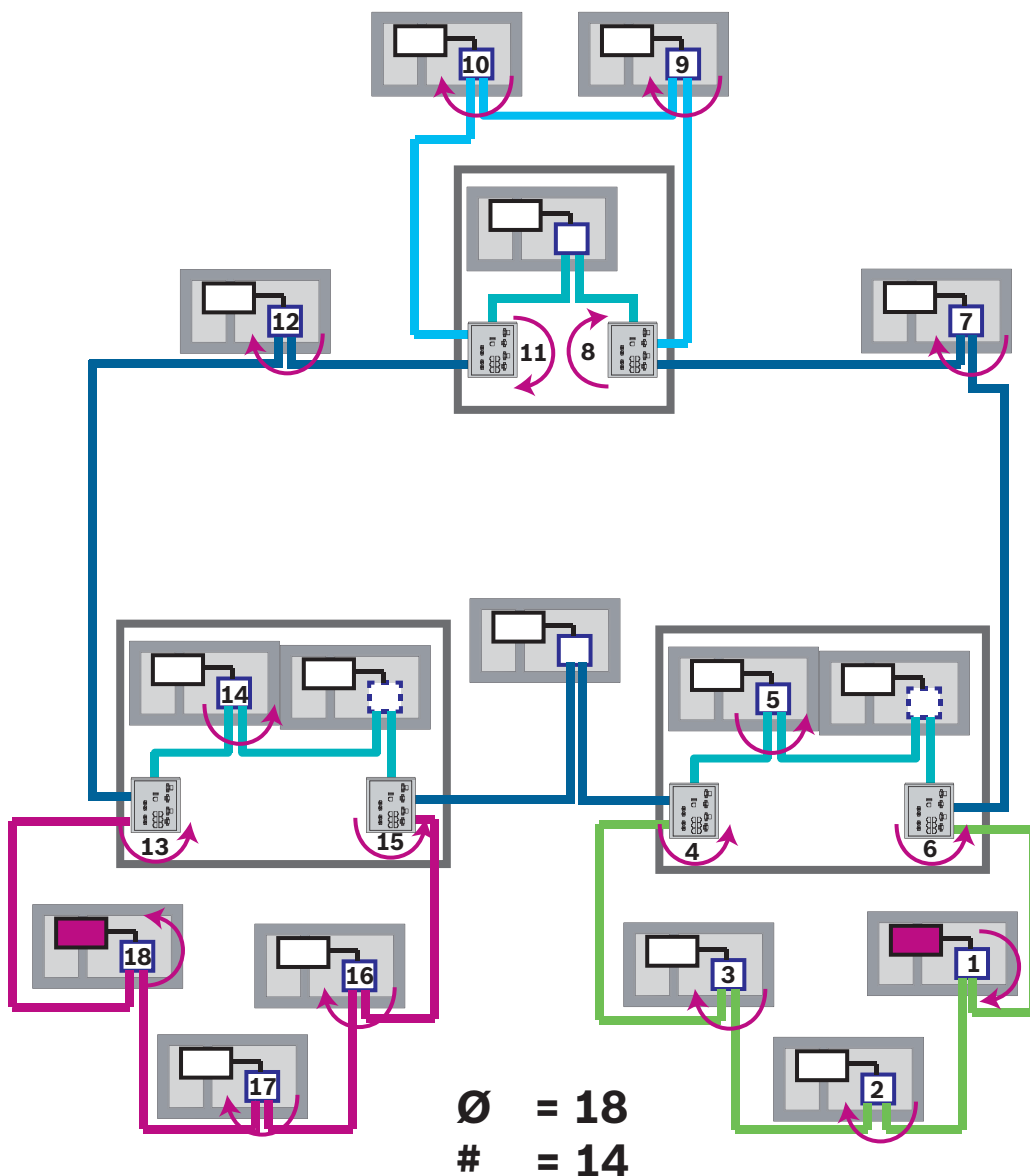


Rysunek 5.1: Pojemność sieci pętli z 2 centralami

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 podpętłe 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

Sieci Ethernet 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 duplex I-VH2G 50/125 μ lub duplex I-VH2G 62.5/125 μ , SC.
Tryb pojedynczy: kabel światłowodowy Ethernet krosowy, wtyczka duplex I-VH2E 9/125 μ , 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 między węzłami musi być mniejsza niż 100 m.



Uwaga!

VdS 2540 – Sieć Ethernet

Jeśli chodzi o centrale łączone w sieci Ethernet, należy pamiętać, że w przypadku instalacji w Niemczech, gdzie wymagana jest zgodność z normą VdS 2540, do wszystkich ścieżek transmisji danych musi być używany kabel światłowodowy. Jedynym wyjątkiem jest tu wnętrze obudowy.

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 podłączenia systemu zarządzania budynkiem, dźwiękowego systemu alarmowego lub systemu integrującego 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, ETH4 można wykorzystać do podłączenia systemu zarządzania budynkiem, dźwiękowego systemu alarmowego lub systemu integrującego.
4. Jeśli centrala nie jest połączona z siecią przez ETH1 i ETH2, każdy z nich może być użyty do podłączenia systemu zarządzania budynkiem, dźwiękowego systemu alarmowego lub systemu integrującego.

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

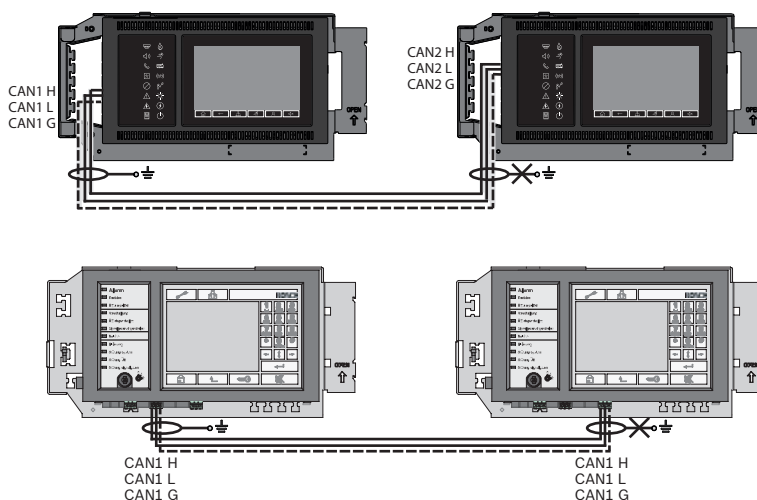
Sieć CAN

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)

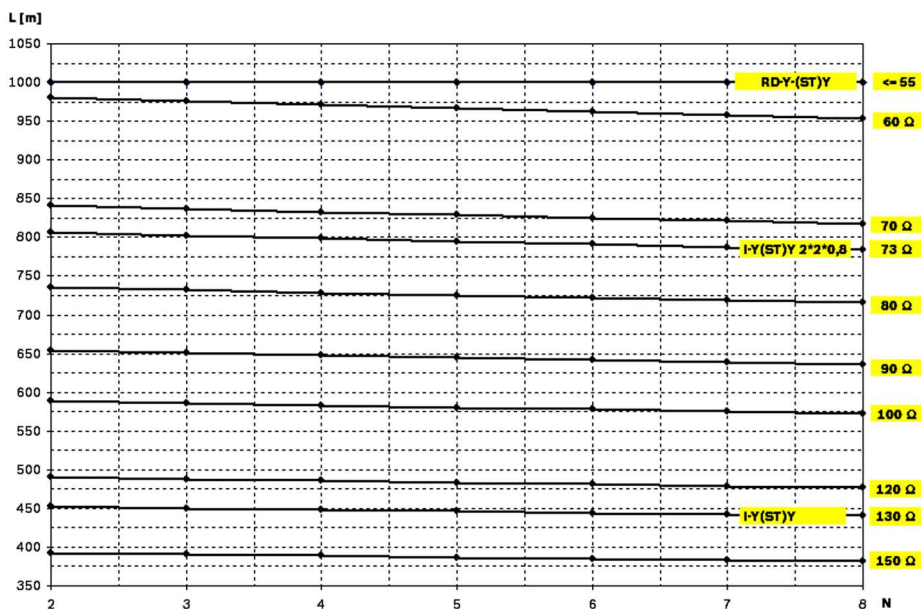
Długość kabla dla połączenia z siecią

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.






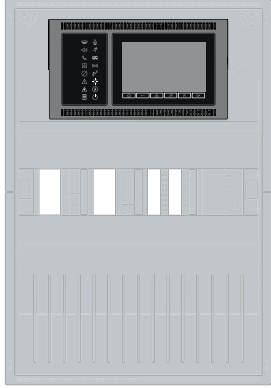
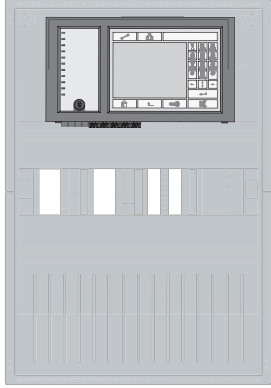
Procedura tworzenia sieci CAN

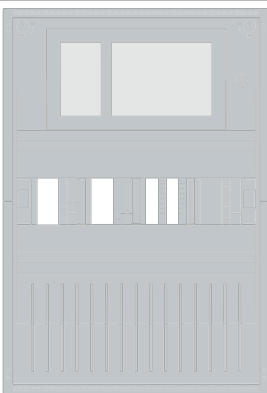
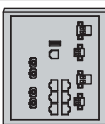



1. Zaplanuj sieć.
2. Utwórz sieć w FSP-5000-RPS.
3. Wydrukuj informacje o sieci i umieść je w bezpiecznym miejscu lub zapisz na komputerze przenośnym.
4. Zainstaluj centrale sygnalizacji pożaru i podłącz je kablami CAN do sieci.
5. Podłącz komputer z aplikacją do programowania FSP-5000-RPS do centrali 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

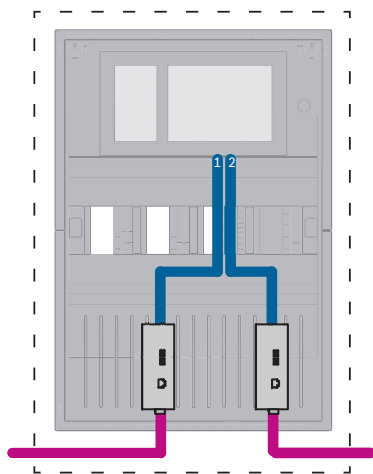
Aby utworzyć sieć centrali odpowiadającą wprowadzonej topologii i usługom łączności, wymagany jest schemat sieci opisany w tym dokumencie.

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

Ikona	Opis
	AVENAR panel lub FPA
	Przełącznik sieci Ethernet jako zewnętrzny switch RSTP (ogólnie switch Ethernet MM)
	Konwerter transmisji
	Bezpieczna brama sieciowa usług Remote Services
	Podłączenie do systemu zarządzania budynkiem, dźwiękowego systemu alarmowego lub systemu integrującego

7.1

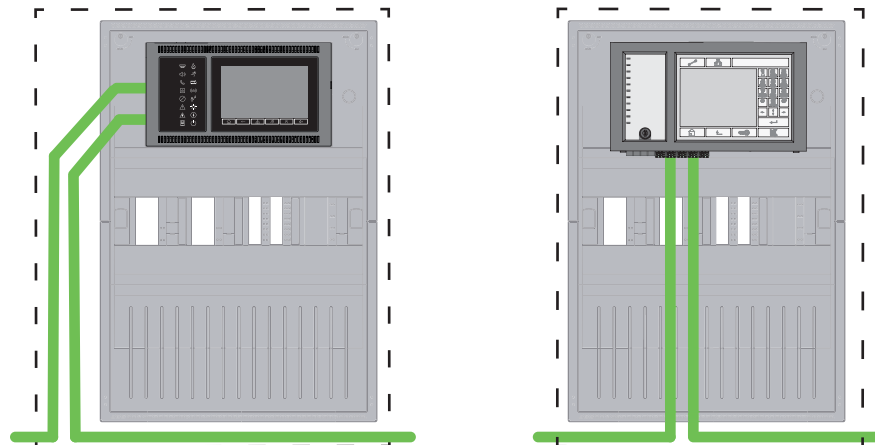
Łączenie central w sieć Ethernet



Rysunek 7.1: Łączenie central w sieć Ethernet

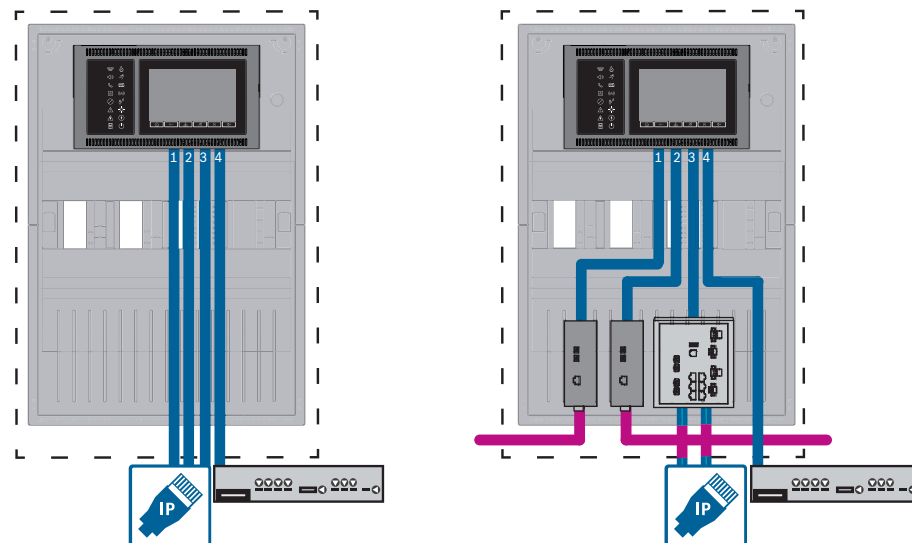
Dla odległości większych niż 100 m wymagane jest użycie konwerterów transmisji. Dla odległości mniejszych niż 100 m użycie konwerterów transmisji może nie być wymagane.

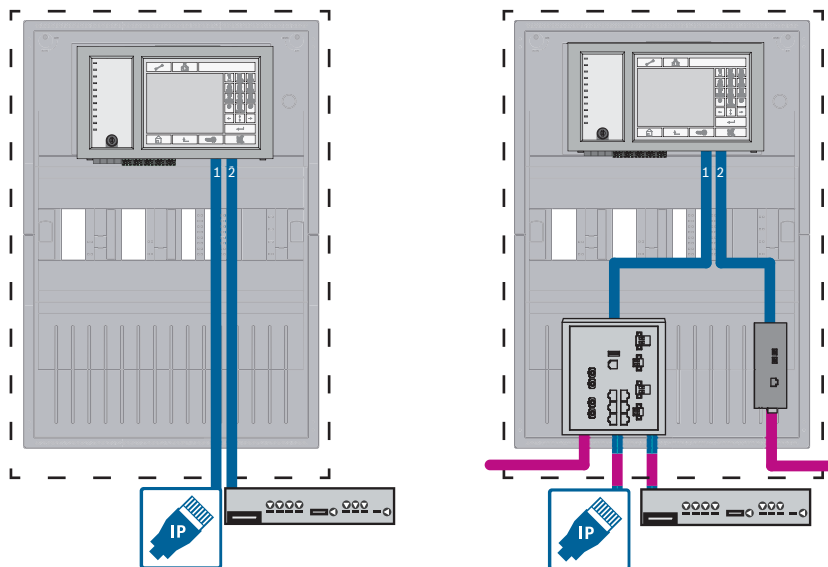
7.2 Łączenie central w sieć CAN



Rysunek 7.2: Łączenie central w sieć CAN

7.3 Podłączanie usług do centrali





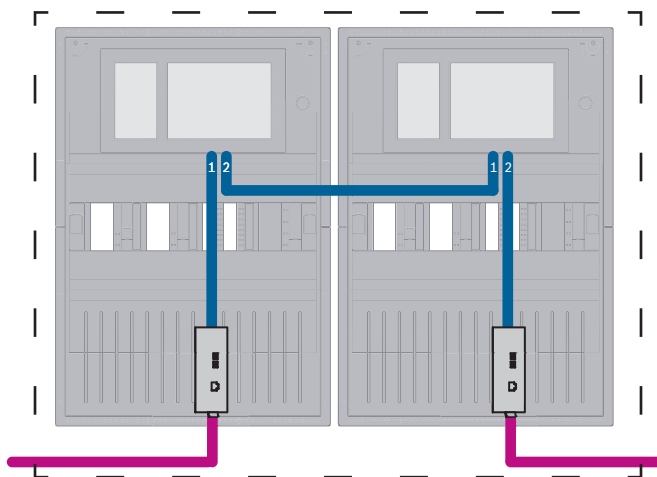
Rysunek 7.3: Po lewej stronie: bez sieci central; po prawej stronie: z siecią central

Przełącznik Ethernet jest wymagany tylko w przypadku połączenia więcej niż dwóch usług z centralą.

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

7.4

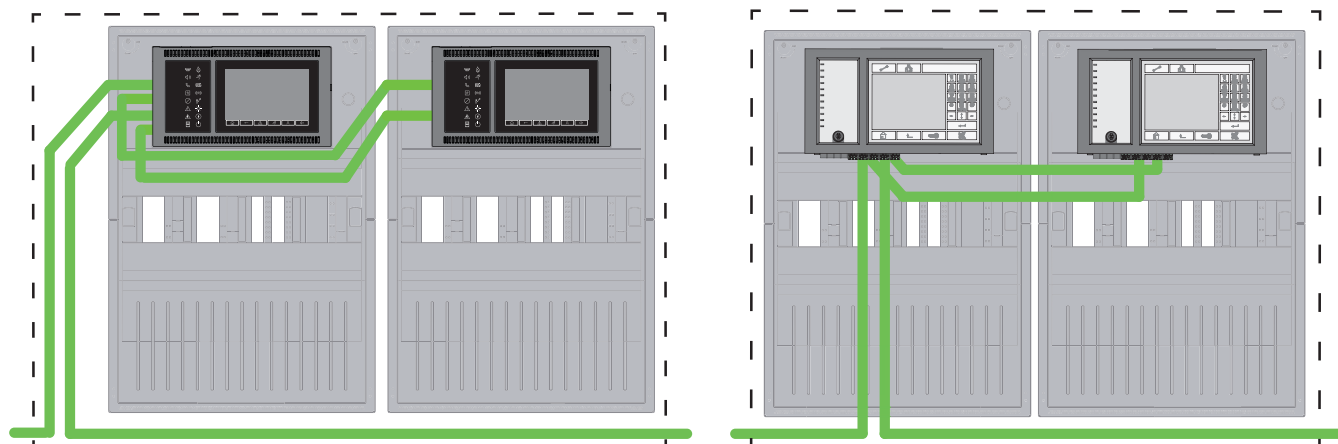
Sieć central w sieci Ethernet z centralami redundantnymi



Rysunek 7.4: Sieć central w sieci Ethernet z centralami redundantnymi

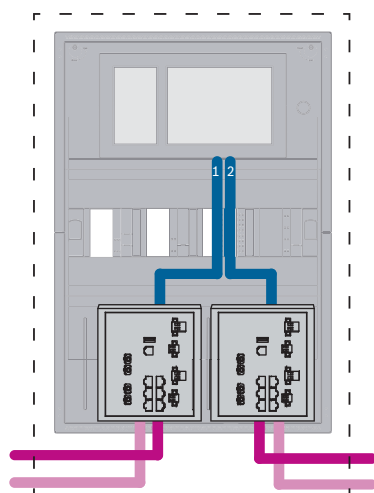
Dla odległości większych niż 100 m wymagane jest użycie konwerterów transmisji. Dla odległości mniejszych niż 100 m użycie konwerterów transmisji może nie być wymagane.

7.5 Sieć central w sieci CAN z centralami redundantnymi



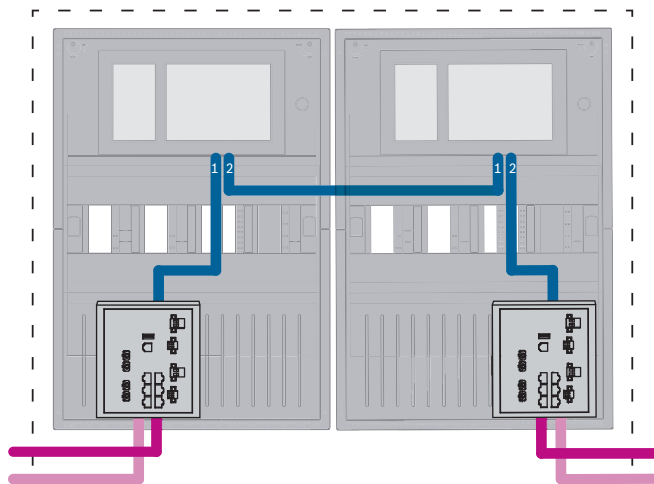
Rysunek 7.5: Sieć central w sieci CAN z centralami redundantnymi

7.6 Połączenie centrali z siecią za pomocą dwóch pętli sieci Ethernet



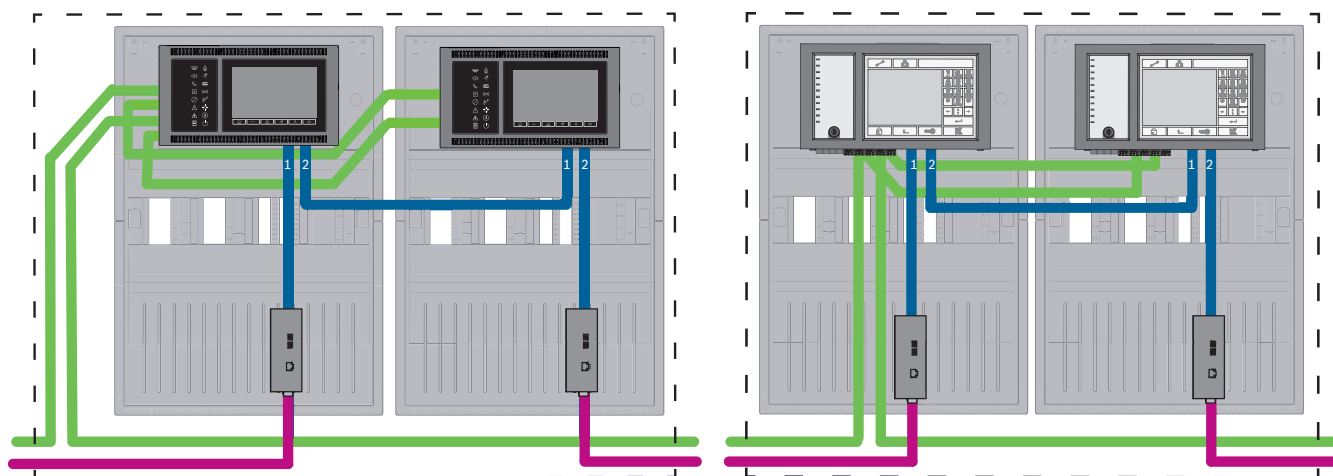
Rysunek 7.6: Połączenia sieci Ethernet

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

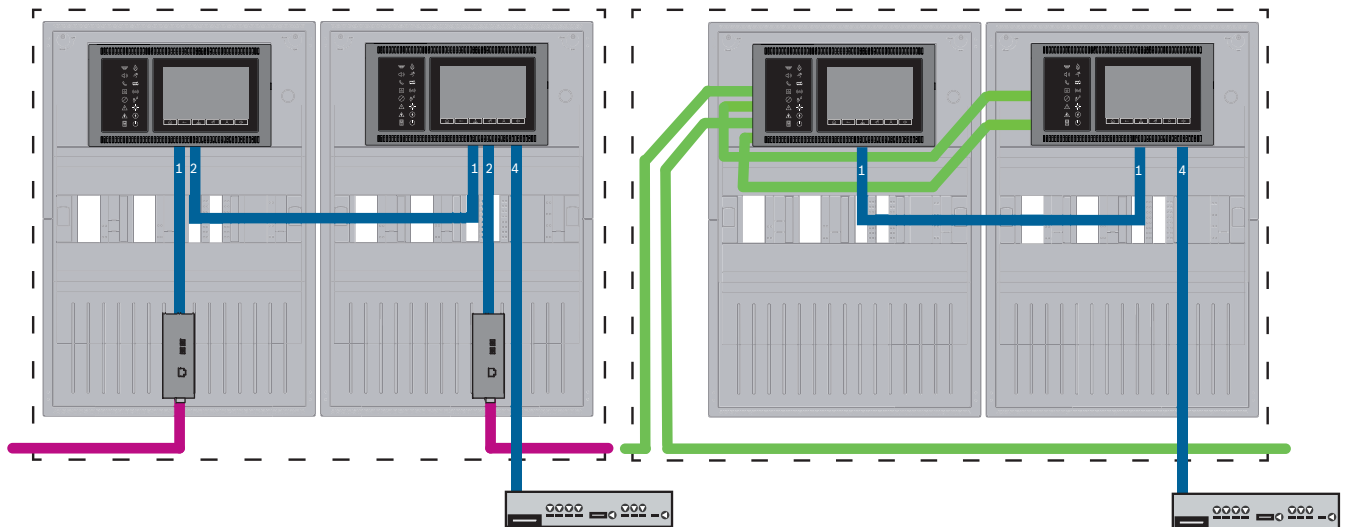
Dla odległości większych niż 100 m wymagane jest użycie konwerterów transmisji. Dla odległości mniejszych niż 100 m użycie konwerterów transmisji może nie być wymagane.

7.9 Podłączanie usług zdalnych do central redundantnymi

Do nadmiarowej centrali FPA lub centrali AVENAR panel można podłączyć bezpieczną bramę sieciową. Z powodów wymienionych poniżej należy rozważyć podłączenie bezpiecznej bramy sieciowej nie do nadmiarowej centrali AVENAR panel, ale do centrali AVENAR panel, która nie pełni roli nadmiarowej:

- Procedura jest rozwiązaniem tymczasowym.
- W przypadku podłączenia do systemu automatyki budynkowej port ETH3 nadmiarowego kontrolera centrali musi być używany i skonfigurowany.

7.9.1 Nadmiarowa centrala AVENAR panel



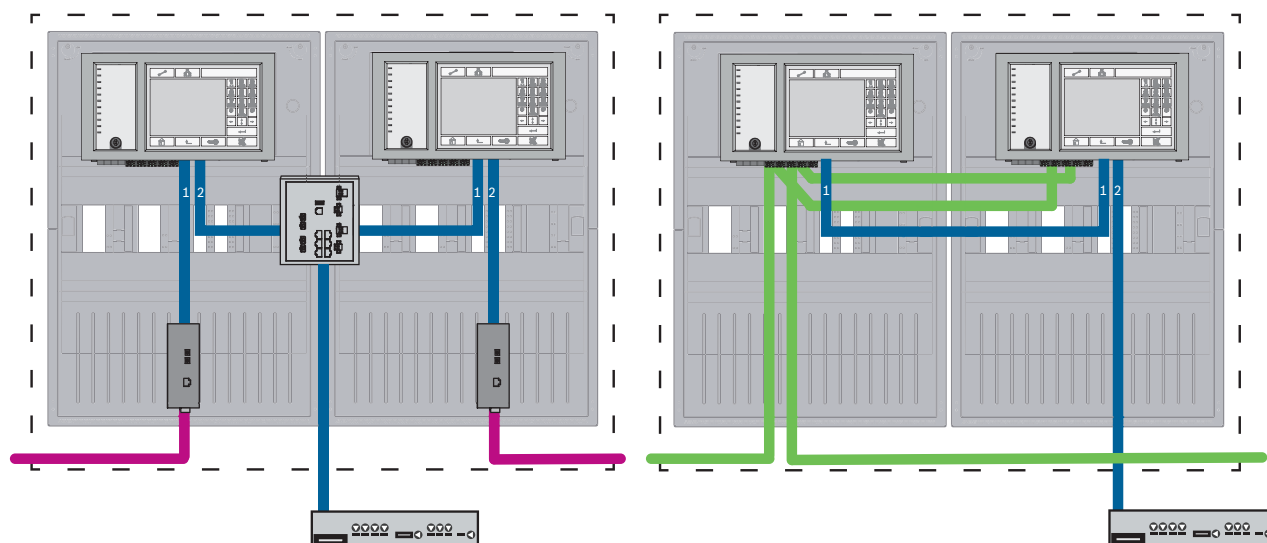
Rysunek 7.9: Po lewej stronie: sieć Ethernet; po prawej stronie: sieć CAN

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

Procedura

1. Bezpieczną bramę sieciową należy podłączyć do portu ETH4 nadmiarowego kontrolera centrali.
2. W sieci CAN należy poprowadzić kabel Ethernet od portu ETH1 do portu ETH1 w nadmiarowym kontrolerze centrali. Skonfigurować ustawienia portu ETH1 w programie FSP-5000-RPS w oknie **Interfejs sieciowy-Ethernet**:
 - W ustawieniu **Typ linii** wybrać **Łącze**
 - Wpisanie w ustawieniu **Połączony z linią numer** numeru linii wyższego niż 0 spowoduje, że połączenie będzie nadzorowane.
3. Dla obu sieci – CAN i Ethernet – należy skonfigurować ustawienia protokołu ETH4 w programie FSP-5000-RPS w oknie **Interfejs sieciowy-Ethernet**:
 - Wpisać wartość 0 w polu **Połączony z linią numer**.
 - Zaznaczyć pole wyboru **Użyj portu**.

7.9.2 Redundantny FPA



Rysunek 7.10: 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 m użycie konwerterów transmisji może nie być wymagane.

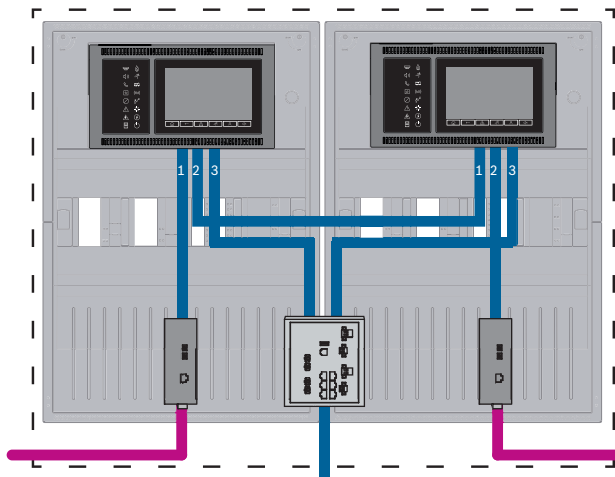
Procedura w sieci CAN

1. Bezpieczną bramę sieciową należy podłączyć do portu ETH2 nadmiarowego kontrolera centrali.
2. W sieci CAN należy poprowadzić kabel Ethernet od portu ETH1 do portu ETH1 w nadmiarowym kontrolerze centrali. Skonfigurować ustawienia portu ETH1 w programie FSP-5000-RPS w oknie **Interfejs sieciowy-Ethernet**:
 - W ustawieniu **Typ linii** wybrać **Łącze**
 - Wpisanie w ustawieniu **Połączony z linią numer** numeru linii wyższego niż 0 spowoduje, że połączenie będzie nadzorowane.
3. Skonfigurować ustawienia portu ETH2 w programie FSP-5000-RPS w oknie **Interfejs sieciowy-Ethernet**:
 - Wpisać wartość 0 w polu **Połączony z linią numer**.
 - Zaznaczyć pole wyboru **Użyj portu**.

7.10 Podłączanie usług ratowania życia do central nadmiarowych

Usługi ratowania życia należy podłączyć do centrali AVENAR panel, która nie jest nadmiarowa:

- Tymczasowego rozwiązania przewidzianego dla usług zdalnych nie można zastosować do połączeń ratowania życia z dźwiękowym systemem alarmowym (VAS over IP) ani z systemem integrującym. Należy zainstalować przełącznik certyfikowany na zgodność z normą EN 54 oraz podłączyć go do głównego kontrolera centrali i nadmiarowego kontrolera centrali.



Rysunek 7.11: Połączenie systemu VAS i systemu integrującego z nadmiarową centralą AVENAR panel

8 Usługi Remote Services

Do Remote Services należą następujące usługi:

- Remote Alert
- Remote Maintenance

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



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.



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.



Przeostroga!

Usługi Remote Services wymagają bezpiecznego połączenia IP. Wymagane jest połączenie z Bosch Remote 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.

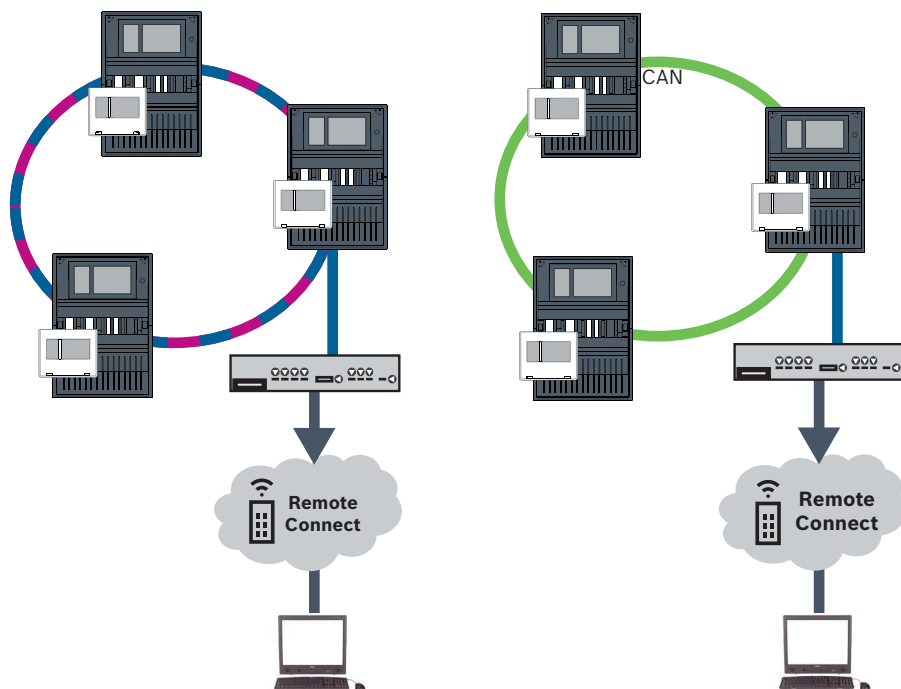
8.1 Warunki wstępne korzystania ze zdalnych usług Remote Services

8.1.1 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. Wyłącznie to połączenie musi być dedykowanym połączeniem Ethernet. 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).
- sieć CAN, w której bezpieczna brama sieciowa jest podłączona do sieci za pośrednictwem portu Ethernet.



Rysunek 8.1: Zdalne połączenie w pętli Ethernet | Zdalne połączenie w pętli CAN

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

Protokół	Domyślny port	Opis
IPsec VPN	UDP 500 i UDP 4500	do Remote Connect

- Podłącz port bezpiecznej bramy sieciowej LAN1 do odpowiedniego portu Ethernet kontrolera centrali za pomocą dołączonego kabla sieciowego CAT5 RJ45. Zauważ możliwe topologie.
- 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 z VPN.

Każda dołączona centrala lub sieć central ma jeden niepowtarzalny identyfikator System ID.



Uwaga!

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

Aby uniemożliwić przesyłanie ruchu multimedialnego 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 podręczniku konfigurowania pracy w sieci.



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.

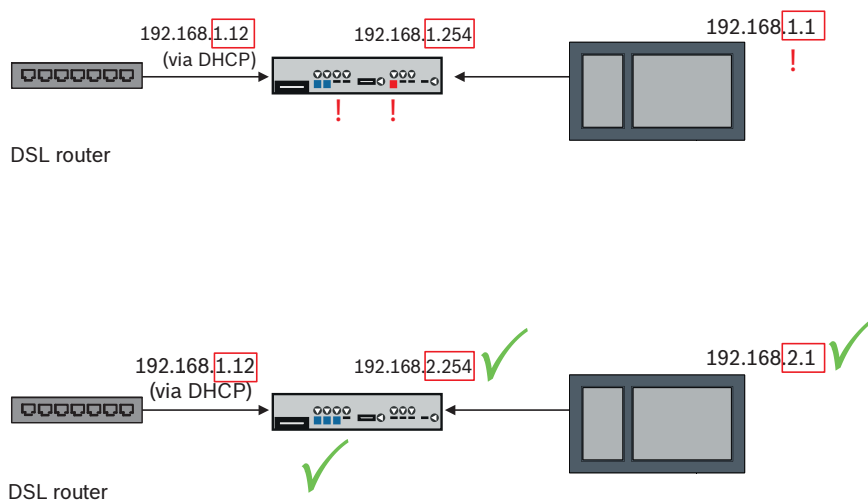


Uwaga!

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

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.

8.1.2

Eksplorator systemu przeciwpożarowego

Aby używać usług Remote Services, trzeba być użytkownikiem dzierżawcy Fire System Explorer (FSE). Niepowtarzalny Remote ID jest przypisany do Twojej firmy.

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 5.12.28 lub wyższej i dostępem do Internetu.

FSE wykorzystuje SingleKey ID. Więcej informacji można znaleźć na stronie poświęconej SingleKey ID: <https://singlekey-id.com>

Tworzenie dzierżawcy FSE

Jeśli nie możesz korzystać z istniejącego dzierżawcy FSE, konieczne będzie utworzenie nowego dzierżawcy na stronie: <https://fse.bosch-nexospace.com/login/>
Może być wymagane zalogowanie się lub założenie konta na stronie SingleKey ID.



Może być też wymagane wyrażenie zgody na warunki umowy i zasady ochrony prywatności. Na podany adres otrzymasz od FSE e-mail z linkiem do aktywacji.

Logowanie w zasobach istniejącego dzierżawcy FSE

Otrzymasz e-mail z zaproszeniem.

1. Kliknij link aktywacyjny w wiadomości e-mail z zaproszeniem.
2. Wybierz dzierżawcę, do którego zasobów chcesz się zalogować. Pokazane są systemy dzierżawcy.

Podłącz do FSP-5000-RPS

Połączenie się z FSP-5000-RPS wymaga utworzenia tokenu dostępowego.

1. W menu FSE kliknij swoją nazwę użytkownika i polecenie **Create Access Token** (Utwórz token dostępowy).
2. Uruchom FSP-5000-RPS.
3. Kliknij ikonę ustawień i wybierz **Options** (Opcje).
4. W oknie **Settings** (Ustawienia) wybierz **Remote Services** (Usługi zdalne).
5. W menu **Account** (Konto), wpisz swój adres e-mail w FSE oraz hasło do FSE, po czym kliknij **OK**.
6. W oknie **Configurations** (Konfiguracja) wybierz swój system.
7. W drzewie nawigacji wybierz **Remote Services** (Usługi zdalne).
8. Wybierz **Remote Portal / Fire System Explorer** na liście **Access Type** (Typ dostępu).
9. Skopiuj wygenerowany token dostępowy
 - do pola **User token** (Token użytkownika), jeśli korzystasz z komputera osobistego, a
 - w innym wypadku do pola **Jednorazowy token**.

8.2 Remote Alert

Za pomocą alertu Remote Alert centrala przesyła informacje o stanie.

Transferowane dane są analizowane wraz z alertem Remote Alert. W przypadku nieoczekiwanego zdarzenia użytkownik zostanie poinformowany za pośrednictwem wiadomości e-mail o otrzymanych alertach.

Usługa Remote Alert jest również dostępna w sieci Private Secure Network.

Elementem Remote Alert jest aplikacja **Remote Fire Safety**. Aplikacja pozwala dostarczać użytkownikom natychmiastowe powiadomienia push na urządzenia mobilne dotyczące alarmów i ostrzeżeń systemowych.

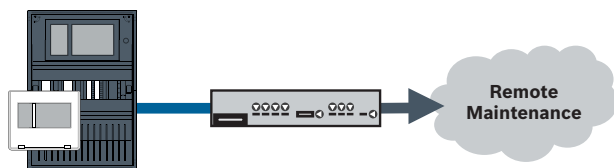
Ponadto użytkownik ma wgląd do historycznych powiadomień, które można udostępniać za e-mailem lub przez komunikatory.

Aplikacja informuje też o stanie systemu, w tym o kondycji, łączności, ważności licencji oraz wymaganiach w zakresie aktualizacji oprogramowania układowego centrali sygnalizacji pożaru.

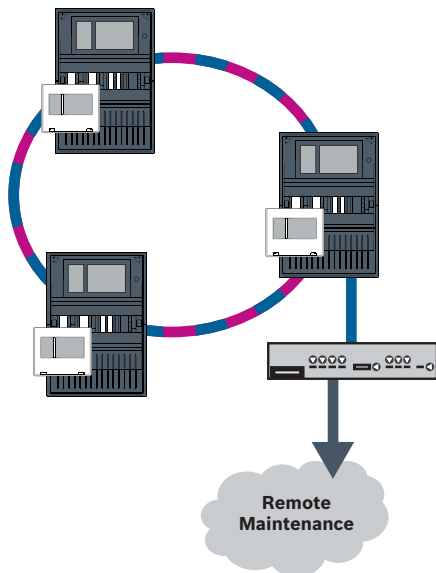
Aplikację można pobrać bezpłatnie ze strony: https://play.google.com/store/apps/details?id=com.bosch.remote_fire_safety&gl=EN lub <https://apps.apple.com/de/app/remote-fire-safety/id1557422840>

8.3 Usługa Remote Maintenance

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



Rysunek 8.2: Usługa Remote Maintenance



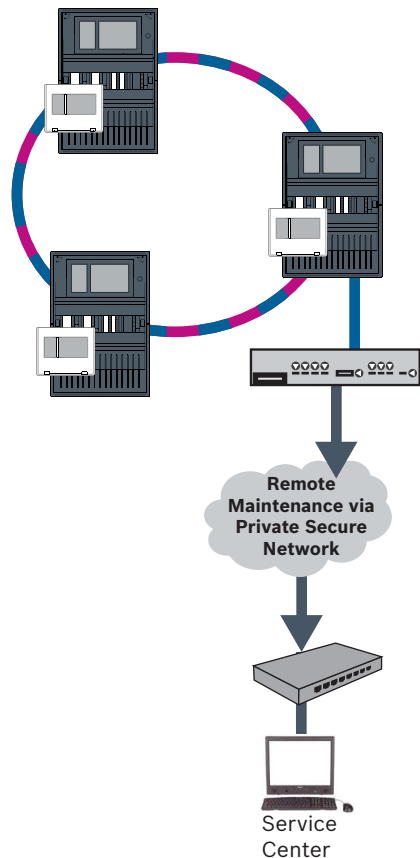
Rysunek 8.3: Usługa Remote Maintenance

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.

Remote Maintenance zbiera dane o odpowiednich urządzeniach LSN i modułach funkcjonalnych. Dane są analizowane i wizualizowane na potrzeby obsługi/konserwacji.

8.4 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).



Rysunek 8.4: 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 podłączenia systemu CMS musi być zaprogramowany oddzielnie.

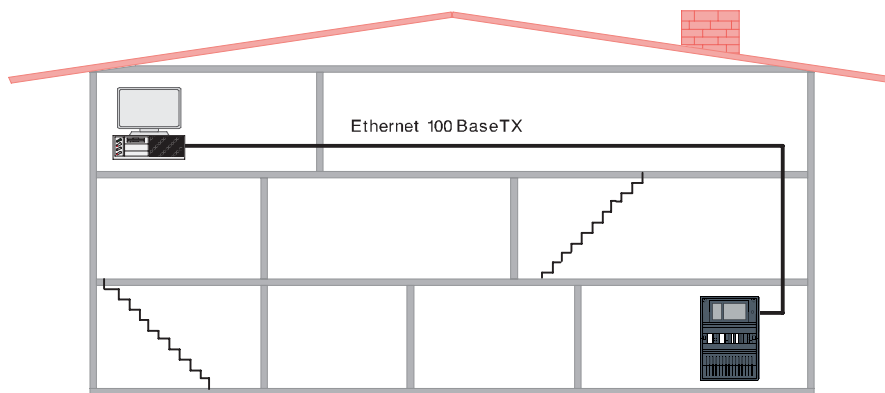
Aby uzyskać informacje o programowaniu ustawień adresu IP i nadmiarowości przełącznika, patrz *Ustawienia przełącznika, Strona 52*. Ze względu na to, że przełącznik jest instalowany w bezpośrednim sąsiedztwie (bez wolnej przestrzeni), nie jest konieczne projektowanie nadmiarowego zasilania. Dlatego też 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.

9 System zarządzania budynkiem

Kontroler centrali wyposażony z licencją premium można podłączyć do systemu zarządzania budynkiem przez interfejs Ethernet przy użyciu jednego z następujących serwerów:

- Serwer FSI: FSI (Fire System Interface) jest zastrzeżonym protokołem komunikacyjnym Bosch. Dostępny jest zestaw SDK, aby wykonać integrację dostosowaną do indywidualnych potrzeb.
- Serwer OPC: OPC (OLE for Process Control) jest standardowym protokołem komunikacyjnym zgodnym z Building Integration System (BIS).
- Serwer BACnet: BACnet (Building Automation i Control Network) jest sztandarowym protokołem komunikacyjnym do łączenia się połączenia z systemem zarządzania budynkiem.



Rysunek 9.1: Łączenie z systemem zarządzania budynkiem

W przypadku podłączania do systemu zarządzania budynkiem za pomocą 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.



Uwaga!

Podczas podłączania systemu zarządzania budynkiem należy przestrzegać instrukcji bezpieczeństwa podanych w części *Bezpieczeństwo*, Strona 5.

Konfiguracja w FSP-5000-RPS

Nawiązanie połączenia z systemem zarządzania budynkiem wymaga utworzenia serwera (OPC server, BACnet server, FSI server) w oprogramowaniu do programowania FSP-5000-RPS.

Konieczne jest skonfigurowanie następujących ustawień zarówno w oprogramowaniu FSP-5000-RPS, jak i na serwerze: adresu węzła logicznego (**Grupa sieciowa i Węzeł sieciowy**), adresu węzła fizycznego (**PNA/RSN**) oraz ustawień IP (**Adres IP i Port**).

Bosch zaleca używanie portu 25000 na potrzeby serwera OPC oraz portu 25001 dla BACnet server lub FSI server.

Należy przypisać serwer do każdej centrali lub zdalnej klawiatury, z której mają być przesyłane statusy. Liczba serwerów, które można przypisać do jednej centrali lub zdalnej klawiatury, jest ograniczona do:

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



Uwaga!

EN 54

Podłączenie systemu zarządzania budynkiem z interfejsem Ethernet jest zgodne z EN 54, jeśli odpowiednie funkcje EN 54 są wykonywane wyłącznie przez centralę sygnalizacji pożaru. Każda metoda kontroli lub administracji zgodna z EN 54 (np. kontrola sygnalizatorów lub wyłączenie elementów) przez system zarządzania budynkiem wymaga osobnej certyfikacji EN 54 całego systemu przez jednostkę certyfikującą.

Przełącznik Ethernet do podłączenia systemu zarządzania budynkiem musi zostać zaprogramowany osobno

Aby uzyskać informacje o programowaniu ustawień adresu IP i nadmiarowości przełącznika Ethernet, patrz *Ustawienia przełącznika, Strona 52*. 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.

Przełączniki do podłączenia systemu zarządzania budynkiem i drugiej pętli muszą być zaprogramowane osobno

Aby uzyskać informacje o programowaniu ustawień adresu IP i nadmiarowości przełącznika Ethernet, patrz *Ustawienia przełącznika, Strona 52*. W przypadku tej topologii użycie wyjść sygnału usterki przełącznika jest konieczne tylko wtedy, jeśli zaprojektowano nadmiarowe zasilanie przełącznika, patrz *Przełącznik Ethernet, Strona 63*.

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 musi być zaprogramowany oddzielnie

Zaprogramuj adres węzła logicznego (**Grupa sieciowa i Węzeł sieciowy**), adres węzła fizycznego (**PNA/RSN**) i ustawienia IP (**Adres IP i Port**).

Firma Bosch zaleca użycie portu 25000 dla interfejsu Ethernet między centralą sygnalizacji pożaru a serwerem.

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

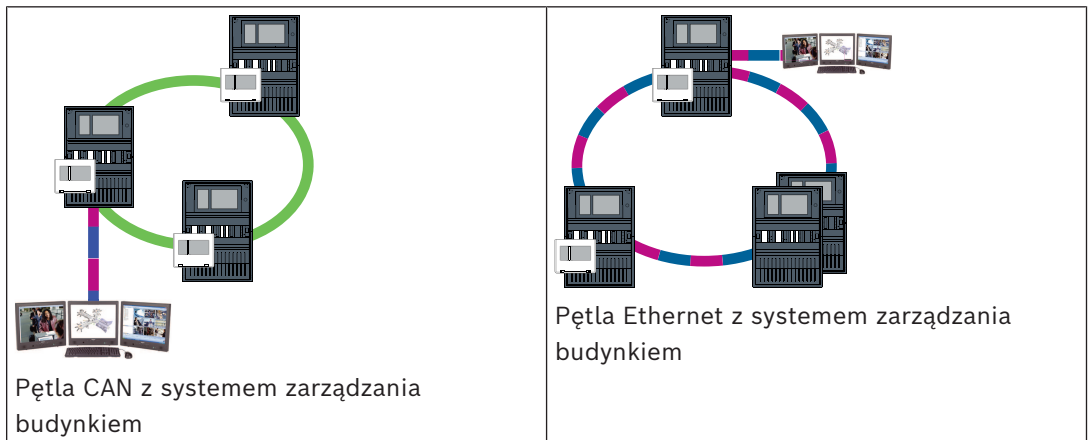


Uwaga!

Szczegółowe informacje na temat instalacji i konfiguracji serwerów BACnet lub OPC można znaleźć w ich instrukcjach dostępnych w katalogu online na www.boschsecurity.com. Instrukcja obsługi serwera FSI jest dostępna w extranet (wymaga posiadania uprawnień dostępu).

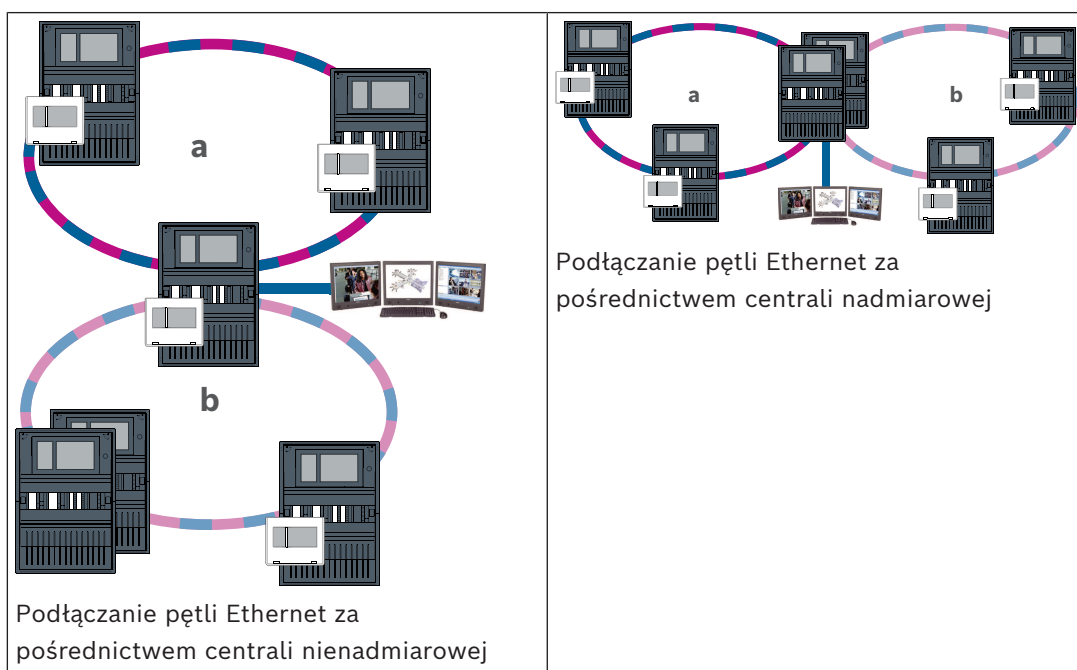
Topologie z systemem zarządzania budynkiem

System zarządzania budynkiem może być podłączony za pomocą kabla Ethernet (miedzianego) lub światłowodu.





W poniższych topologiach pętla a jest szkieletem. Pętla b jest podpętlą.



10

Inteligentne łącze bezpieczeństwa

W tym rozdziale opisano rozwiązanie techniczne bezpiecznego interfejsu sieci Ethernet między centralami sygnalizacji pożaru Bosch a dźwiękowymi systemami alarmowymi Bosch. Smart Safety Link jest najbardziej niezawodnym i bezpiecznym interfejsem łączącym wykrywanie pożaru i dźwiękowy system ostrzegawczy (VAS). Smart Safety Link oferuje wyjątkową elastyczność i opcje rozbudowy.

System dwukierunkowej wymiany danych ustanawia nadzorowane połączenie między centralą sygnalizacji pożaru a systemem VAS. Zarówno centrala sygnalizacji pożaru, jak i system VAS sygnalizują komunikat o usterce, gdy połączenie zostanie przerwane. W przypadku przerwania połączenia użytkownik może ręcznie rozpocząć ewakuację całego budynku za pośrednictwem stacji wywoławczej systemu VAS. Przerwanie interfejsu nie powoduje automatycznej ewakuacji budynku. Po ponownym ustanowieniu interfejsu centrala sygnalizacji pożaru automatycznie synchronizuje bieżący stan alarmu z systemem VAS. W przypadku pożaru centrala sygnalizacji pożaru może automatycznie uruchamiać komunikaty

głosowe za pomocą wirtualnych wyzwalaczy VAS, które są aktywowane przez reguły skonfigurowane w FSP-5000-RPS. Centrala sygnalizacji pożaru generuje komunikat nadzoru, gdy zdarzenie ewakuacji zostanie uruchomione przez system VAS. Usterka systemu VAS wygeneruje komunikat o błędzie w interfejsie użytkownika centrali sygnalizacji pożaru. W graficznym interfejsie użytkownika centrali AVENAR panel operator może wyciszyć komunikaty emitowane przez centralę. Operator może wyświetlić przegląd stanu wszystkich wyzwalaczy wirtualnych. Każdy wirtualny wyzwalacz może być oznaczony jednoznaczną etykietą wskazującą lokalizację i typ komunikatu. Charakterystyczny kolor odzwierciedla stan każdego wirtualnego wyzwalacza. Operator z uprawnieniami użytkownika L2 może ręcznie uruchomić i zatrzymać komunikat głosowy w wybranym wyzwalaczu wirtualnym. Systemy PAVIRO i Praesideo można podłączać do central FPA i AVENAR panel. Ze względu na topologię sieciową system PRAESENSA wymaga interfejsu z szyfrowaną komunikacją danych. AVENAR panel zawierająca oprogramowanie układowe kontrolera centrali w wersji 4.x może się łączyć tylko z systemem PRAESENSA. Funkcję Smart Safety Link używającą sieci Ethernet wprowadzono w oprogramowaniu układowym kontrolera centrali w wersji 2.11 oraz w oprogramowaniu FSP-5000-RPS w wersji 4.3.

**Ostrzeżenie!**

Zagrożenia dla bezpieczeństwa podczas korzystania z sieci Ethernet
Nie łączyć urządzeń systemu PRAESENSA z centralami FPA-5000/FPA-1200 za pośrednictwem funkcji Smart Safety Link ze względu na zagrożenia dla bezpieczeństwa powodowane przez sieć Ethernet.

**Uwaga!**

Dźwiękowy system ostrzegawczy podłączony do centrali AVENAR
Każda centrala sygnalizacji pożaru fizycznie podłączona do dźwiękowego systemu ostrzegawczego poprzez interfejs Smart Safety Link wymaga licencji premium.

**Uwaga!**

Dźwiękowy system alarmowy połączony z centralą FPA
Każda centrala przeciwpożarowa, która jest fizycznie podłączona do dźwiękowego systemu alarmowego za pośrednictwem funkcji Smart Safety Link i zawiera oprogramowanie układowe w wersji 3.x, nie wymaga klucza licencji na ten system dźwiękowy.

10.1

Jeden bezpośredni interfejs do systemu VAS

Centralę przeciwpożarową i dźwiękowy system alarmowy można połączyć za pomocą jednego kabla TX Ethernet.

**Uwaga!**

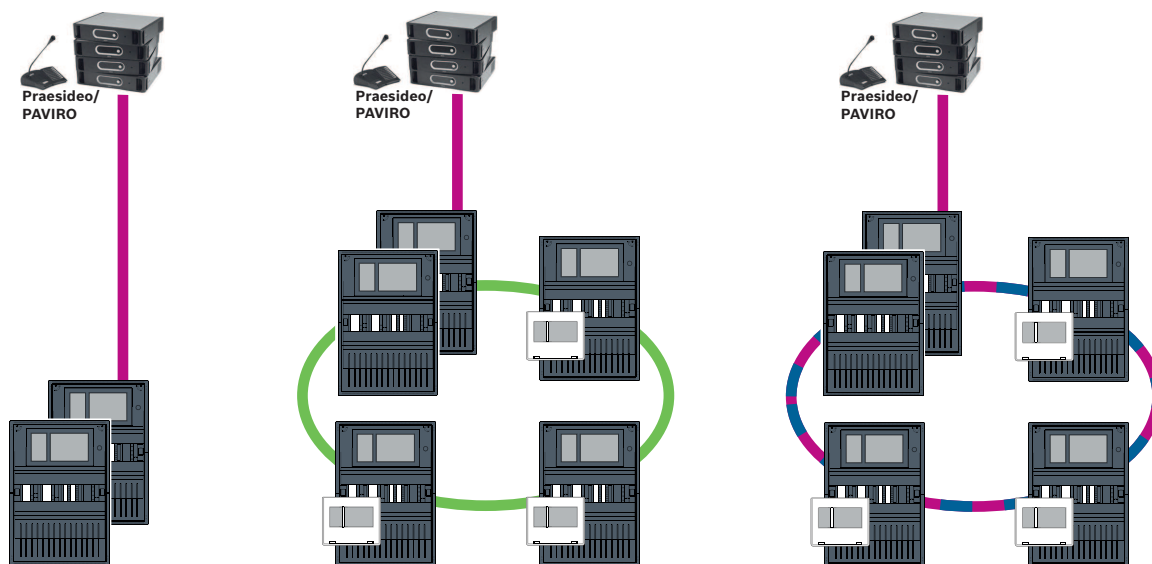
VdS 2540
Dźwiękowy system alarmowy musi być zamontowany w jednej płaszczyźnie z centralą sygnalizacji pożaru w tym samym pomieszczeniu. W przeciwnym razie nie zostaną spełnione wymagania dyrektywy VdS 2540 dla torów transmisji danych.

10.1.1

Praesideo i PAVIRO

Centrale AVENAR panel i FPA można podłączać bezpośrednio do dedykowanego otwartego portu sieci Ethernet w kontrolerze systemu Praesideo (PRS-NCO-3) lub PAVIRO (PVA-4CR12).

Otwartego interfejsu można używać dla pojedynczej centrali lub sieci central.



Rysunek 10.1: Jeden bezpośredni interfejs do systemu Praesideo|PAVIRO



Uwaga!

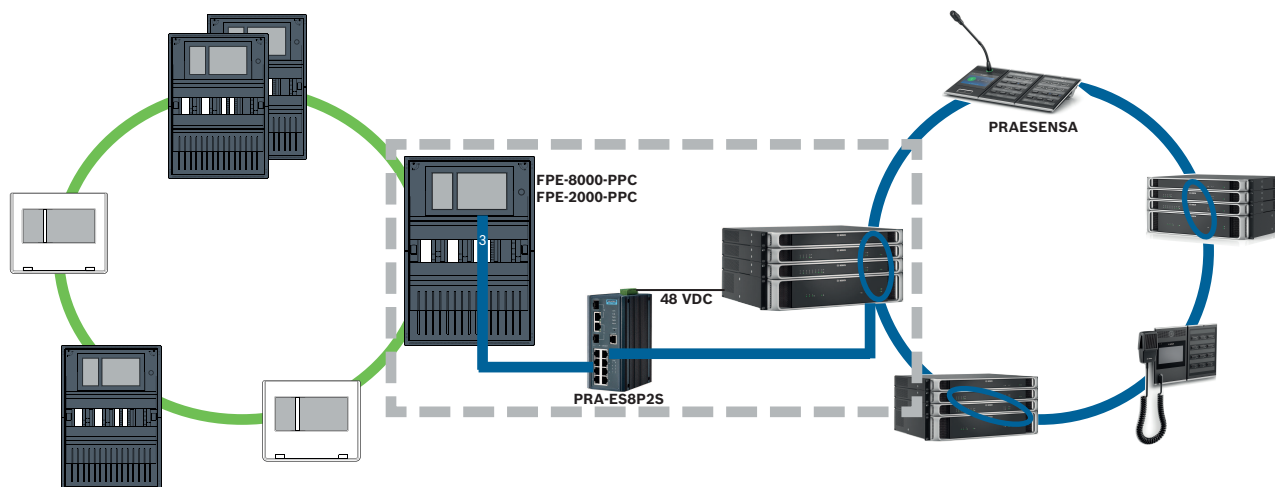
Jeśli kontroler centrali MPC-xxxx-B ma służyć do bezpośredniego połączenia z systemem Praesideo/PAVIRO, wymagane jest użycie połączeniowego kabla krosowego, ponieważ ani Praesideo/PAVIRO, ani MPC-xxxx-B nie obsługują Auto-MDI(X).

10.1.2

PRAESENSA

PRAESENSA to sieciowy dźwiękowy system alarmowy wykorzystujący sieć IP do transmisji dźwięku i sterowania.

W celu podłączenia centrali AVENAR panel do systemu PRAESENSA zawsze należy używać przełącznika sieci PRA-ES8P2S wyposażonego w 8 interfejsów PoE i 2 interfejsy SFP.



Rysunek 10.2: Podłączenie systemu PRAESENSA do centrali AVENAR panel

Przeostroga!

Zagrożenia dla bezpieczeństwa podczas korzystania z sieci Ethernet

Do łączenia systemu PRAESENSA z centralą FPA-5000/FPA-1200 nie należy stosować funkcji Smart Safety Link. W całej sieci można używać tylko central AVENAR panel i klawiatur AVENAR keypad 8000. W celu podłączenia systemu PRAESENSA do centrali FPA-5000/FPA-1200 należy wykorzystać styki przełącznika opisane w dokumencie TI2363/2021. W przeciwnym razie sieć Ethernet będzie narażona na ataki.



**Uwaga!**

Podłączanie systemu PRAESENSA do centrali AVENAR panel

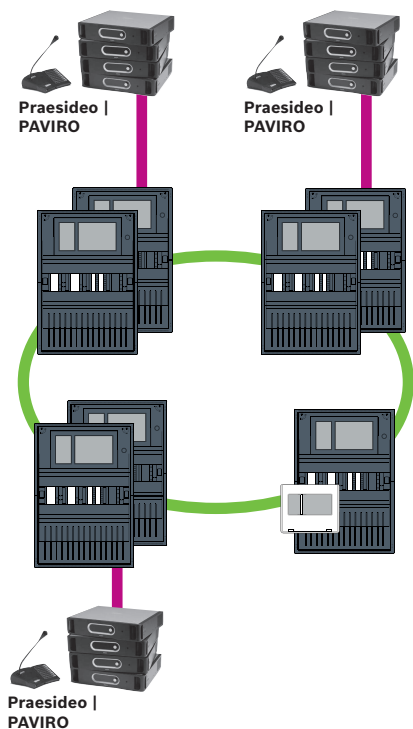
- Przetłaczniaka PRA-ES8P2S należy używać wyłącznie dla funkcji Smart Safety Link. Do portów przetłaczniaka sieci Ethernet wyposażonego w 8 interfejsów PoE i 2 interfejsy SFP można podłączyć tylko kontroler systemu PRA-SCL, bez żadnych innych urządzeń systemu PRAESENSA. Przetłaczniaka sieci Ethernet wyposażonego w 8 interfejsów PoE i 2 interfejsy SFP nie wolno używać do łączenia z systemem zarządzania budynkiem, systemem integrującym, bezpieczną bramą sieciową dla usług zdalnych itd.
- Do łączenia z systemem PRAESENSA za pośrednictwem funkcji Smart Safety Link należy użyć centrali zawierającej tylko jeden kontroler centrali. W połączeniach z systemem PRAESENSA za pośrednictwem funkcji Smart Safety Link nadmiarowość kontrolera centrali nie jest jeszcze obsługiwana. Centrale w sieci, które nie są bezpośrednio podłączone do systemu PRAESENSA, mogą zawierać nadmiarowe kontrolery centrali.
- Do sieci central należy użyć topologii magistrali CAN. Nie łączyć central przez sieć Ethernet.
- Wszystkie centrale AVENAR panel i klawiatury AVENAR keypad 8000 w sieci muszą mieć oprogramowanie układowe centrali w wersji 4.x.

Procedura

1. Zamontować przetłaczniak sieci PRA-ES8P2S Ethernet w szafie typu Rack systemu PRAESENSA. Zamontować kontroler PRA-SCL w jednej płaszczyźnie z centralą AVENAR panel w tym samym pomieszczeniu. Nie umieszczać przetłaczniaka sieci Ethernet PRA-ES8P2S w obudowie centrali AVENAR panel.
2. Przetłaczniak PRA-ES8P2S musi otrzymywać zasilanie z systemu PRAESENSA.
3. Skonfigurować przetłaczniak sieci Ethernet PRA-ES8P2S:
 - zezwolić tylko na komunikację w formie emisji pojedynczej między kontrolerem FPE-8000-PPC a kontrolerem systemu PRAESENSA
 - zablokować całą komunikację w formie multicast
 - wyłączyć obsługę protokołu RSTP
4. Sprawdzić tryb pracy systemu PRAESENSA, musi to być DHCP. Funkcja Smart Safety Link nie obsługuje trybu Zeroconf.
5. Podłączyć kontroler PRAESENSA za pomocą jednego kabla sieci Ethernet (protokół RSTP jest wyłączony).
6. W konfiguracji funkcji Smart Safety Link w centrali AVENAR panel w programie FSP-5000-RPS zaznaczyć opcję **Szyfrowane VAS over IP**.

10.2**Wiele bezpośrednich interfejsów do systemu VAS**

W sieci CAN każdą centralę sygnalizacji pożaru można podłączyć do jednego dźwiękowego systemu alarmowego. Zastosować bezpośrednie połączenie z interfejsem zgodnie z opisem w punkcie *Jeden bezpośredni interfejs do systemu VAS, Strona 45*.



Rysunek 10.3: Wiele bezpośrednich interfejsów do systemu VAS

Dla każdego węzła, w którym ma zostać dezaktywowane połączenie z centralą przez sieć przy użyciu protokołu IP, wykonać następującą procedurę w programie FSP-5000-RPS:

1. Zaznaczyć węzeł, w którym ma zostać wyłączone połączenie z centralą przez sieć.
2. Wybierz **Użyj ustawień Ethernet**.
3. Usuń zaznaczenie opcji **łączenie central w sieci IP**.
4. Kliknij **Zastosuj**.

10.3

System VAS zintegrowany w sieci central połączonych przez Ethernet

Jeżeli systemy Praesideo i PAVIRO są zintegrowane w sieci central, to dźwiękowy system alarmowy ma nadmiarowy tor transmisyjny. Nadmiarowy tor umożliwia zamontowanie centrali sygnalizacji pożaru i dźwiękowego systemu alarmowego w osobnych pomieszczeniach.

Obecnie nie można zintegrować systemu PRAESENSA w sieci central połączonych przez Ethernet.



Uwaga!

VdS 2540

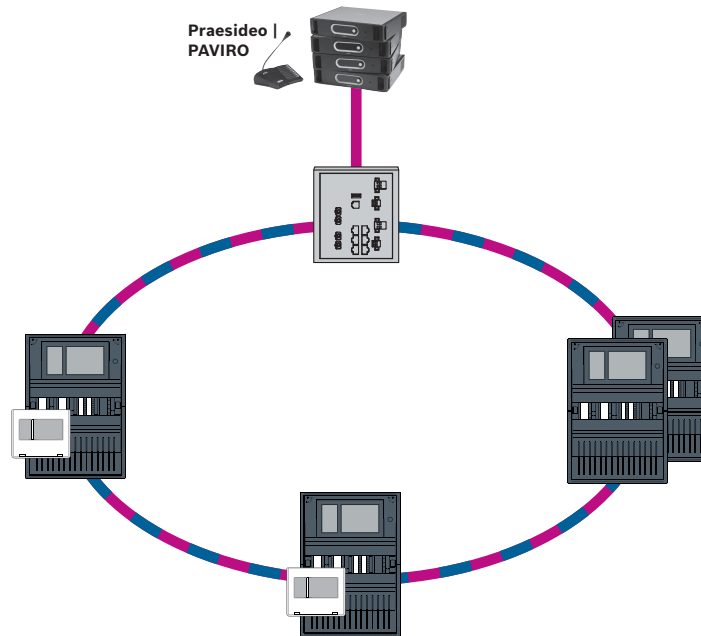
Dźwiękowy system alarmowy musi być zamontowany w jednej płaszczyźnie z centralą sygnalizacji pożaru w tym samym pomieszczeniu. W przeciwnym razie nie zostaną spełnione wymagania dyrektywy VdS 2540 dla torów transmisji danych.



Uwaga!

VdS 2540 – Sieć Ethernet

Jeśli chodzi o centrale łączone w sieci Ethernet, należy pamiętać, że w przypadku instalacji w Niemczech, gdzie wymagana jest zgodność z normą VdS 2540, do wszystkich ścieżek transmisji danych musi być używany kabel światłowodowy. Jedynym wyjątkiem jest tu wnętrze obudowy.



Rysunek 10.4: System VAS zintegrowany w sieci central połączonych przez Ethernet
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 podręczniku konfigurowania pracy w sieci.

System sygnalizacji pożaru musi zasilać przełącznik Ethernet.

11 System integrujący

Aby nawiązać połączenie z systemem integrującym, trzeba utworzyć serwer UGM server w oprogramowaniu FSP-5000-RPS.

Konieczne jest skonfigurowanie następujących ustawień zarówno w oprogramowaniu FSP-5000-RPS, jak i w systemie integrującym: adresu węzła logicznego (**Grupa sieciowa i Węzeł sieciowy**), adresu węzła fizycznego (**PNA/RSN**) oraz ustawień IP (**Adres IP i Port**). Firma Bosch zaleca użycie portu 25001 dla interfejsu Ethernet między centralą sygnalizacji pożaru a systemem integrującym.

Należy przypisać serwer do każdej centrali lub zdalnej klawiatury, z której mają być przesyłane statusy. Liczba serwerów, które można przypisać do jednej centrali lub zdalnej klawiatury, jest ograniczona do:

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

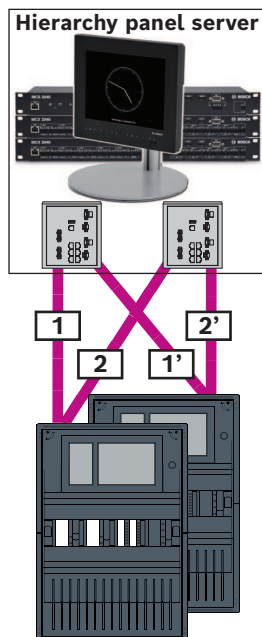


Uwaga!

Wszystkie kontrolery centrali i serwery systemu integrującego 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.

Aby podłączyć centralę do systemu integrującego, należy symulować strukturę fizyczną sieci w FSP-5000-RPS. Dotyczy to również numerów linii łączących kontroler centrali i przełączniki systemu integrującego.



Rysunek 11.1: Przykład numeracji linii w systemie integrującym

12

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.
 - Sprawdzone, czy do dyspozycji są dodatkowe składniki, które mają być zainstalowane, takie jak przełączniki Ethernet i konwertery transmisji, oraz ich okablowanie z sąsiednimi centralami.
 - Sprawdzone, czy do dyspozycji jest topologia sieci, która ma być zainstalowana.
 - Wszystkie ustawienia nadmiarowości sieci są zaplanowane i do dyspozycji.

12.1

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.

**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, duplex I-VH2G 50/125 μ lub duplex I-VH2G 62.5/125 μ , wtyczka SC.

Tryb pojedynczy: sieciowy kabel światłowodowy Ethernet, duplex I-VH2E 9/125 μ

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!**

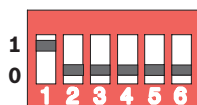
W przypadku wielomodowych konwerterów transmisji maksymalna długość odcinka transmisji za pośrednictwem FX wynosi 2000 m.

W przypadku jednomodowych konwerterów transmisji maksymalna długość odcinka transmisji za pośrednictwem FX wynosi 40 km.

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

**Uwaga!**

Zmiany ustawień przelaznika DIP w konwerterach transmisji mogą być wykonywane wyłącznie po odłączeniu zasilania.



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

12.2 Montaż przetwornika 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 przetwornika Ethernet FPM-5000-KES(F.01U.260.523).

12.3 Ustawienia przetwornika

Aby umożliwić użycie przetworników w sieci, trzeba je zaprogramować.

Podłącz komputer przenośny do sieci i za pomocą dostarczonego przez producenta oprogramowania HiDiscovery wykonaj wstępne programowanie przetworników. Postępując się tym oprogramowaniem, wyszukaj przetworniki w sieci. Kliknij dwukrotnie przetwornik, aby go wybrać, i przypisz do niego adres IP.

Po wstępnym zaprogramowaniu adresu IP można za pomocą przeglądarki internetowej wywołać interfejs użytkownika umożliwiający konfigurację przetwornika.



Uwaga!

Dokładny opis instalacji i konfiguracji przetworników można znaleźć w instrukcji producenta.

Dane dostępowe:

Użytkownik: admin

Hasło: private

Za pomocą przeglądarki wywołaj interfejs użytkownika, aby wybrać ustawienia dla przetworników.

Skonfiguruj następujące ustawienia:

- *Przypisanie adresu IP, Strona 52,*
- *Programowanie ustawień nadmiarowości, Strona 53.*

Ponadto dostępne są ustawienia opcjonalne, np.:

- *Programowanie przekaźnika usterki, Strona 54,*
- *Programowanie monitoringu połączeń, Strona 54,*
- *Jak włączyć śledzenie IGMP, Strona 55.*

12.3.1 Przypisanie adresu IP



Uwaga!

Praktyczna wskazówka:

Jeśli konfiguracja sieciowa to umożliwia, w części adresów IP dotyczących urządzenia dla przetworników należy używać liczb większych niż 200 (xxx.xxx.xxx.200). Zapewni to lepsze odróżnienie od identyfikatora adresu IP hosta.

Przykład:

Przetwornik 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).

12.3.2

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 protokołu): RSTP
- Protocol configuration (Konfiguracja protokołu): 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).

12.3.3 Programowanie przekaźnika usterki

**Uwaga!**

Programowanie przekaźnika usterki jest wymagane tylko w przypadku zastosowań spełniających co najmniej jeden z poniższych warunków:

Istnieje połączenie pomiędzy 2 switchami. 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).

12.3.4 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** (Przełącz 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** (Przełącz 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).

12.3.5

Priorytet QoS

W przypadku używania przełączników do wymiany danych pomiędzy sieciami central sygnalizacji pożaru i systemem integrującym konieczne jest ustawienie priorytetu QoS w przełącznikach systemu integrującego.

W przypadku systemu integrującego UGM-2040 zmień ustawienia w menu QoS/Priorität -> Global 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).

12.3.6

Jak włączyć śledzenie IGMP

Aby zabezpieczyć wysyłanie ruchu multimediami pozwalającego spełnić normę EN 54-2 do innych systemów podłączonych do urządzenia Ethernet Switch (dźwiękowego systemu alarmowego zintegrowanego z siecią central połączonych przez Ethernet, systemu Remote Connect itp.), należy włączyć 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 multimediami na zapytania IGMP queries (np. 3 sekundy).
5. Wybierz opcję **Discard** (Odrzuć) dla pakietów z nieznanymi adresami multimediami.
6. Wybierz opcję **Send to Query and registered Ports** (Wysyłaj do portów zapytania i zarejestrowanych) dla pakietów o znanych adresach multimediami.
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.

12.4

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:

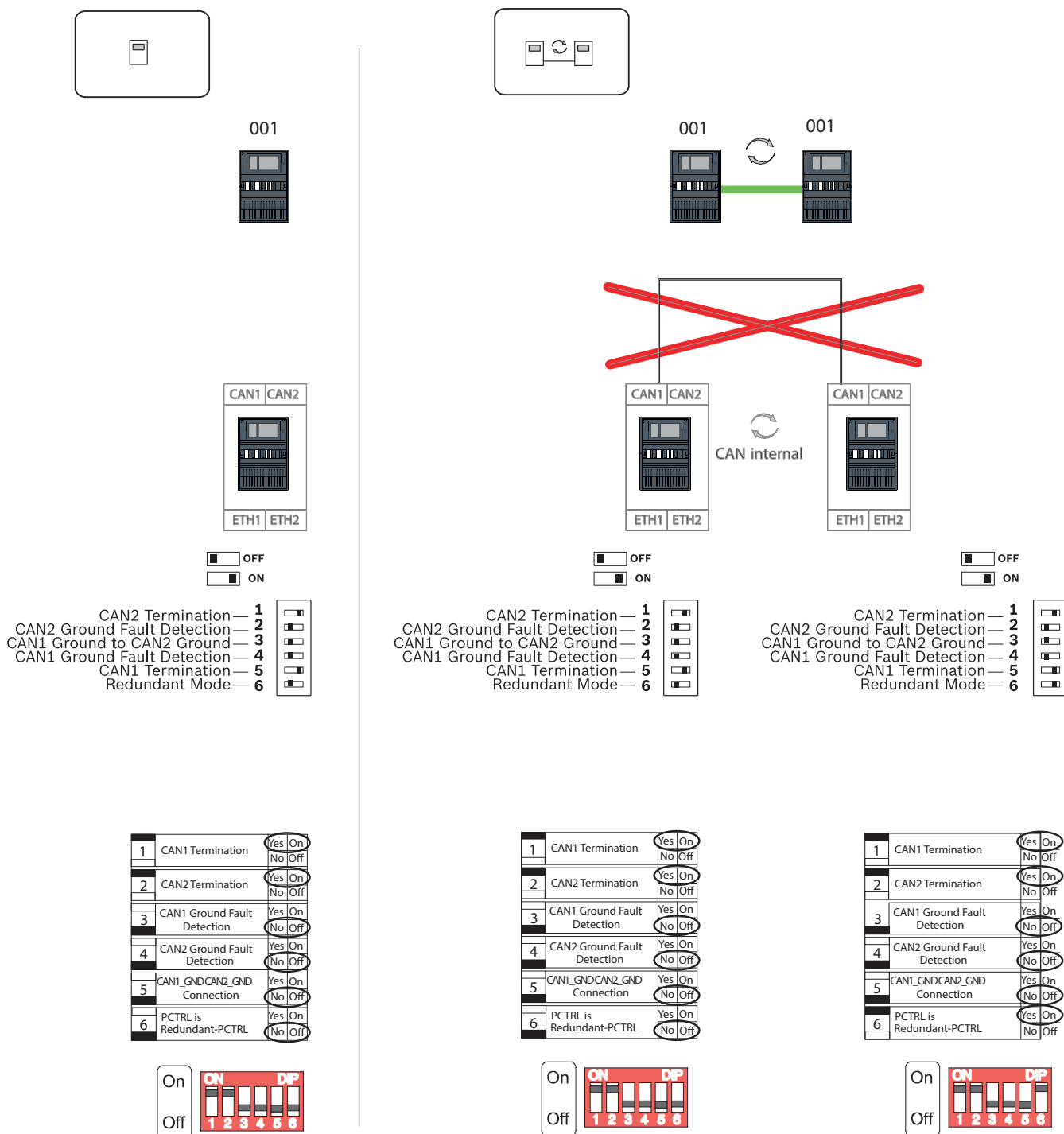
- ▶ Ustaw na mechanicznym switchu obrotowym z tyłu centrali wartość RSN i zanotuj ją na etykiecie poniżej tego switcha.

Konfiguracja topologii

Przełączniki DIP służące do ustawienia topologii są umieszczone z tyłu.

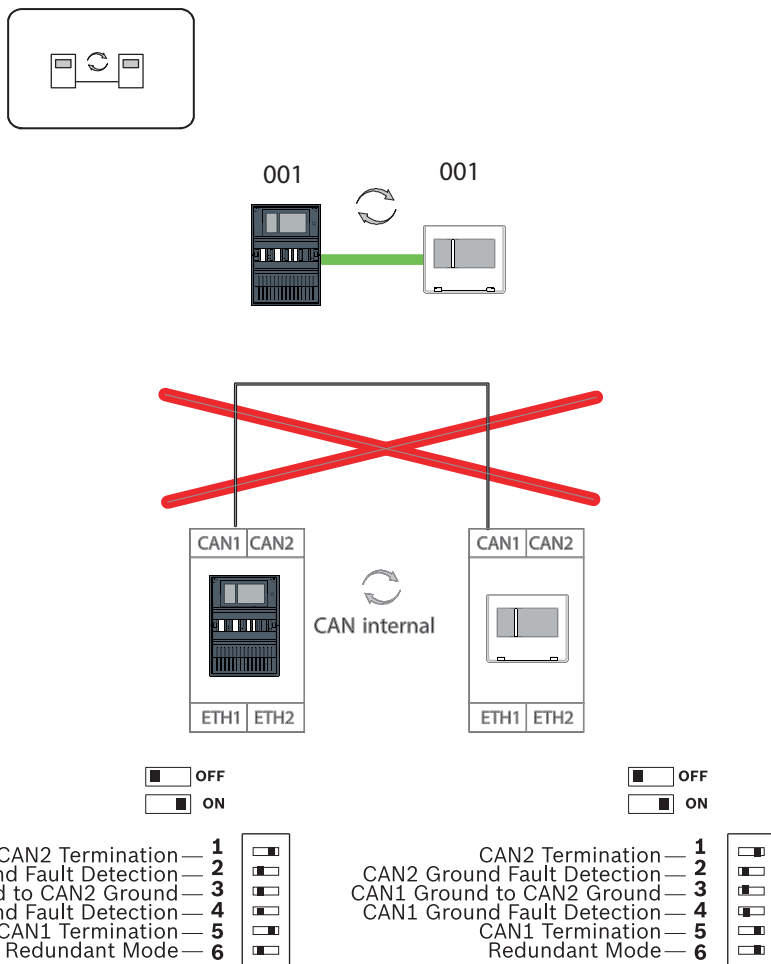
- ▶ Należy oznaczyć wybrane ustawienie na etykiecie w pobliżu przełączników DIP.

Samodzielna centrala i redundanta samodzielna centrala



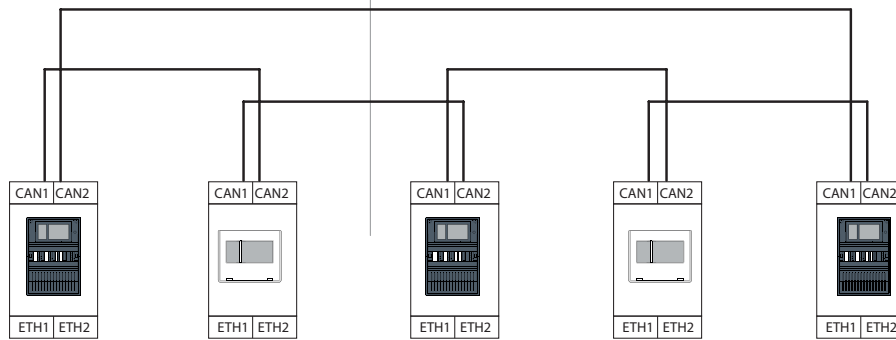
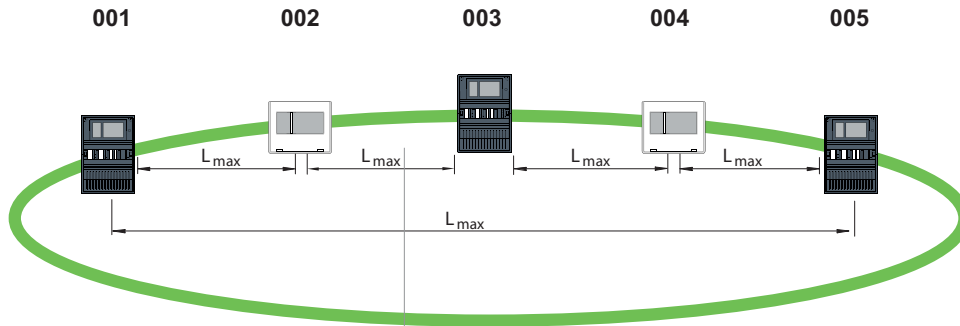
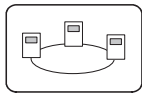
Rysunek 12.1: Ustawienia switcha DIP dla centrali autonomicznej (u góry: AVENAR, u dołu: FPA, po lewej: zwykła, po prawej: redundanta)

Wyniesiona klawiatura jako redundantna centrala



Rysunek 12.2: Ustawienia switcha DIP do konfiguracji klawiatury wyniesionej jako centrali redundantnej (tylko AVENAR)

Pętla



Legend for switch configurations:

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

1	<input type="checkbox"/>
2	<input type="checkbox"/>
3	<input type="checkbox"/>
4	<input type="checkbox"/>
5	<input type="checkbox"/>
6	<input type="checkbox"/>

- 1 CAN2 Termination
- 2 CAN2 Ground Fault Detection
- 3 CAN1 Ground to CAN2 Ground
- 4 CAN1 Ground Fault Detection
- 5 CAN1 Termination
- 6 Redundant Mode

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

1	CAN1 Termination	Yes/On	No/Off
2	CAN2 Termination	Yes/On	No/Off
3	NA	Yes/On	No/Off
4	NA	Yes/On	No/Off
5	CAN1_GND/CAN2_GND Connection	Yes/On	No/Off
6	NA	Yes/On	No/Off

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

1	CAN1 Termination	Yes/On	No/Off
2	CAN2 Termination	Yes/On	No/Off
3	NA	Yes/On	No/Off
4	NA	Yes/On	No/Off
5	CAN1_GND/CAN2_GND Connection	Yes/On	No/Off
6	NA	Yes/On	No/Off

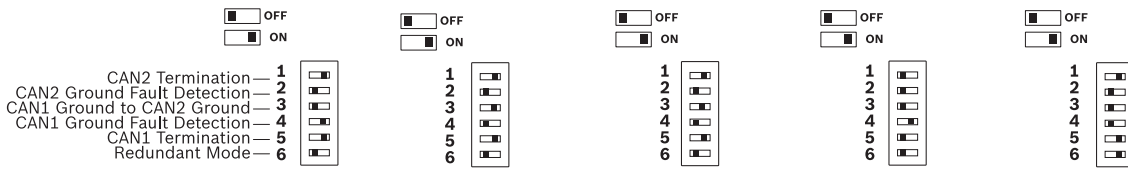
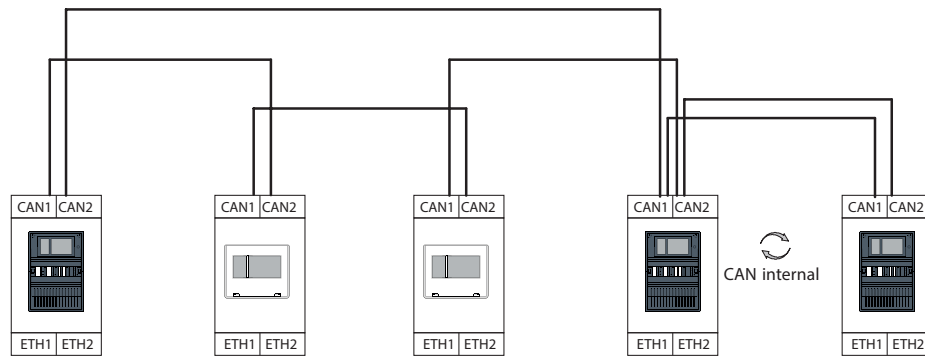
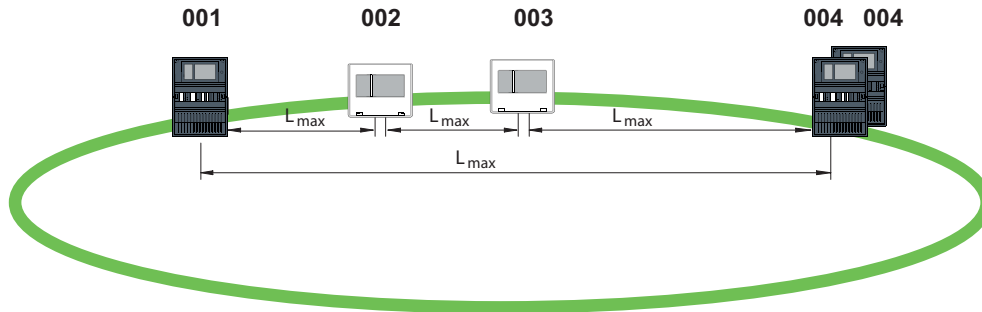
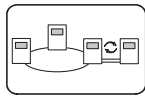
1	CAN1 Termination	Yes/On	No/Off
2	CAN2 Termination	Yes/On	No/Off
3	CAN1 Ground Fault Detection	Yes/On	No/Off
4	CAN2 Ground Fault Detection	Yes/On	No/Off
5	CAN1_GND/CAN2_GND Connection	Yes/On	No/Off
6	PCTRL is Redundant-PCTRL	Yes/On	No/Off

Legend for DIP switches:

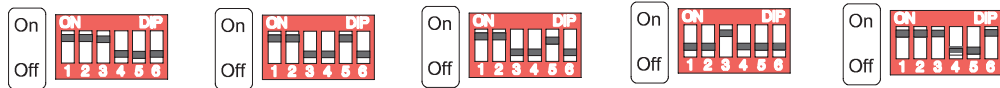
- On (red bar)
- Off (white bar)

Rysunek 12.3: Ustawienia switcha DIP dla pętli (u góry: AVENAR, u dołu: FPA)

Łęta z centralami redundantnymi

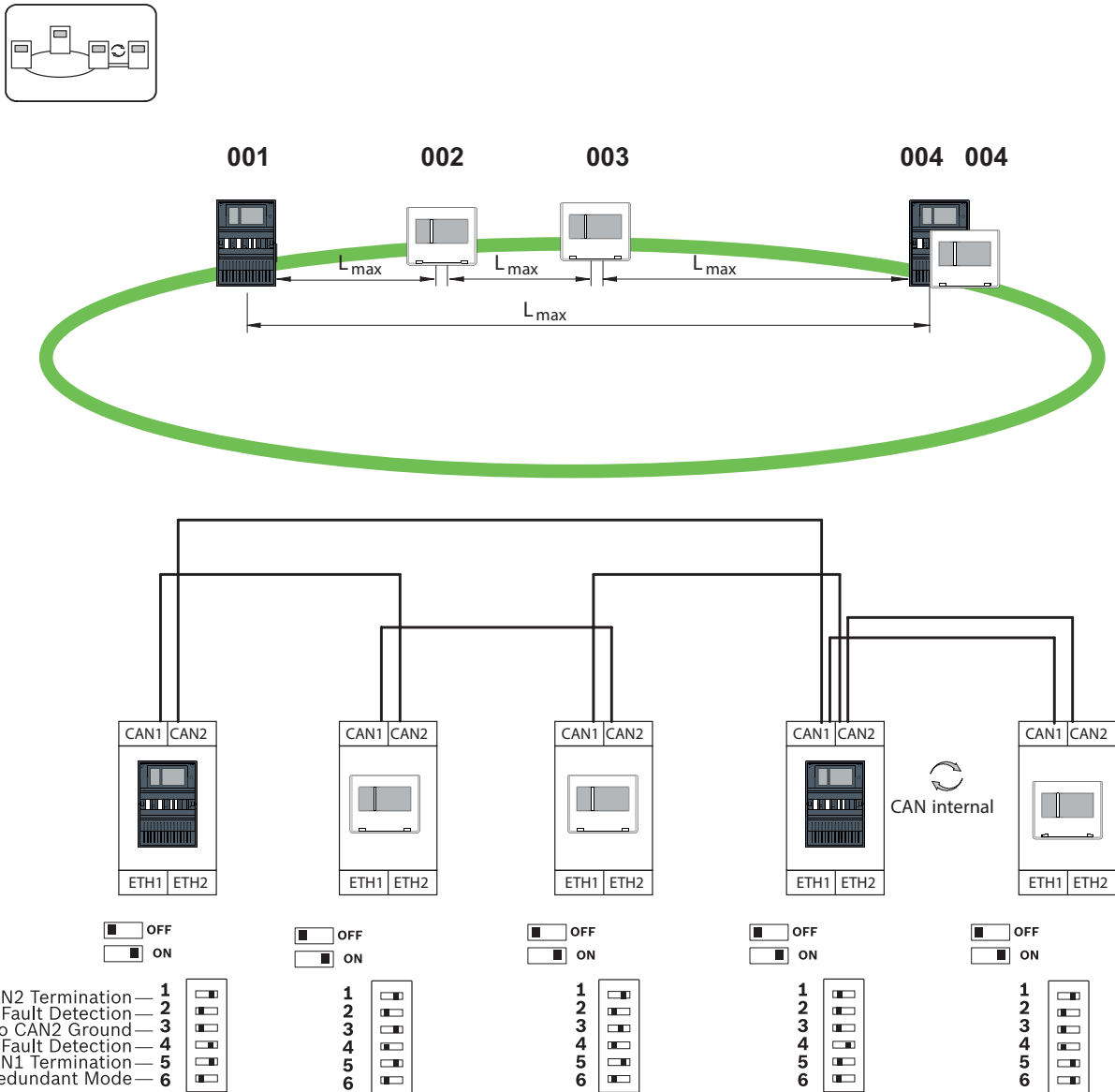


1	CAN1 Termination	Yes/On	No/Off	1	CAN1 Termination	Yes/On	No/Off	1	CAN1 Termination	Yes/On	No/Off	1	CAN1 Termination	Yes/On	No/Off
2	CAN2 Termination	Yes/On	No/Off	2	CAN2 Termination	Yes/On	No/Off	2	CAN2 Termination	Yes/On	No/Off	2	CAN2 Termination	Yes/On	No/Off
3	CAN1 Ground Fault Detection	Yes/On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



Rysunek 12.4: Ustawienia switcha DIP dla łęty z redundantnymi centralami (u góry: AVENAR, u dołu: FPA)

Pętla z klawiaturą wyniesioną jako centralą redundantną



Rysunek 12.5: Ustawienia switcha DIP do pętli z klawiaturą wyniesioną (tylko AVENAR)

13 Okablowanie Ethernet

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 modułu kontrolera akumulatorów lub zasilania zewnętrznego 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!**

Sieci Ethernet 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

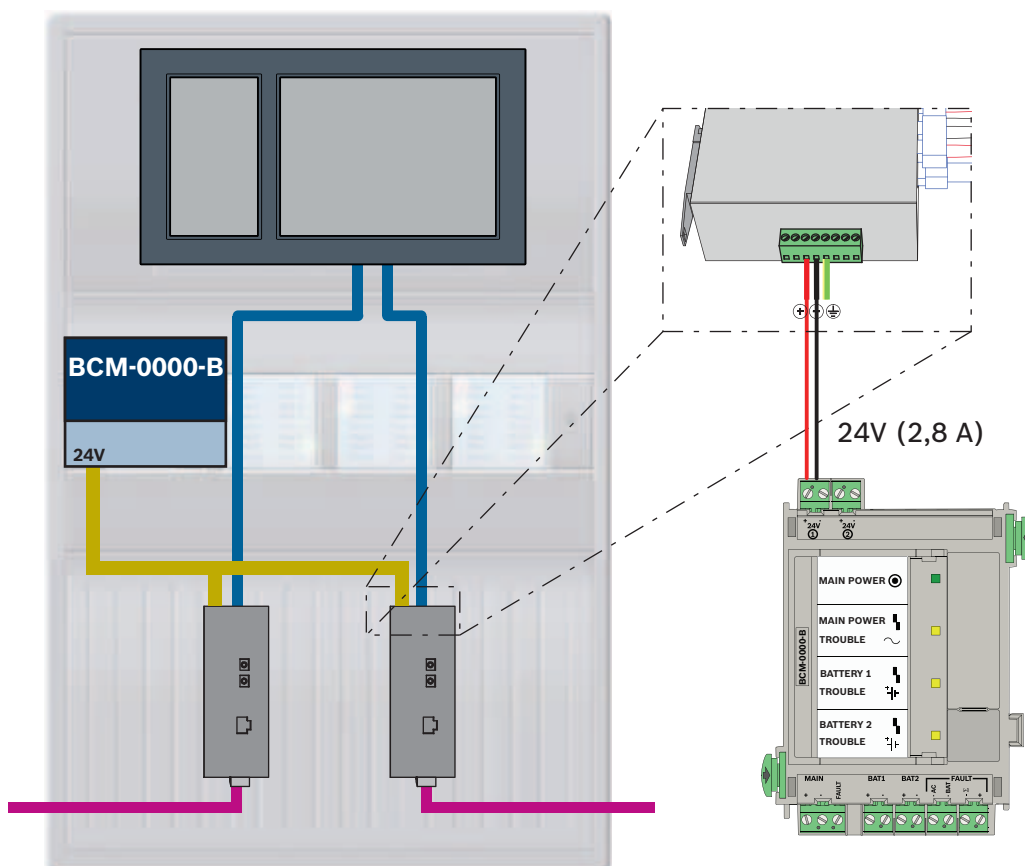
Tryb multi-mode: sieciowy kabel światłowodowy Ethernet, duplex I-VH2G 50/125 μ lub duplex I-VH2G 62.5/125 μ , wtyczka SC.

Tryb pojedynczy: sieciowy kabel światłowodowy Ethernet, duplex I-VH2E 9/125 μ , wtyczka SC.



Należy pamiętać o minimalnym promieniu zgięcia określonym w specyfikacji kabla.

13.1**Konwerter transmisji****Połączenie konwerterów transmisji****Uwaga!**

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



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

Ikona	Opis
	Transmisja usterki
	Konwerter transmisji

13.2

Przełącznik Ethernet

Połączenie switcha

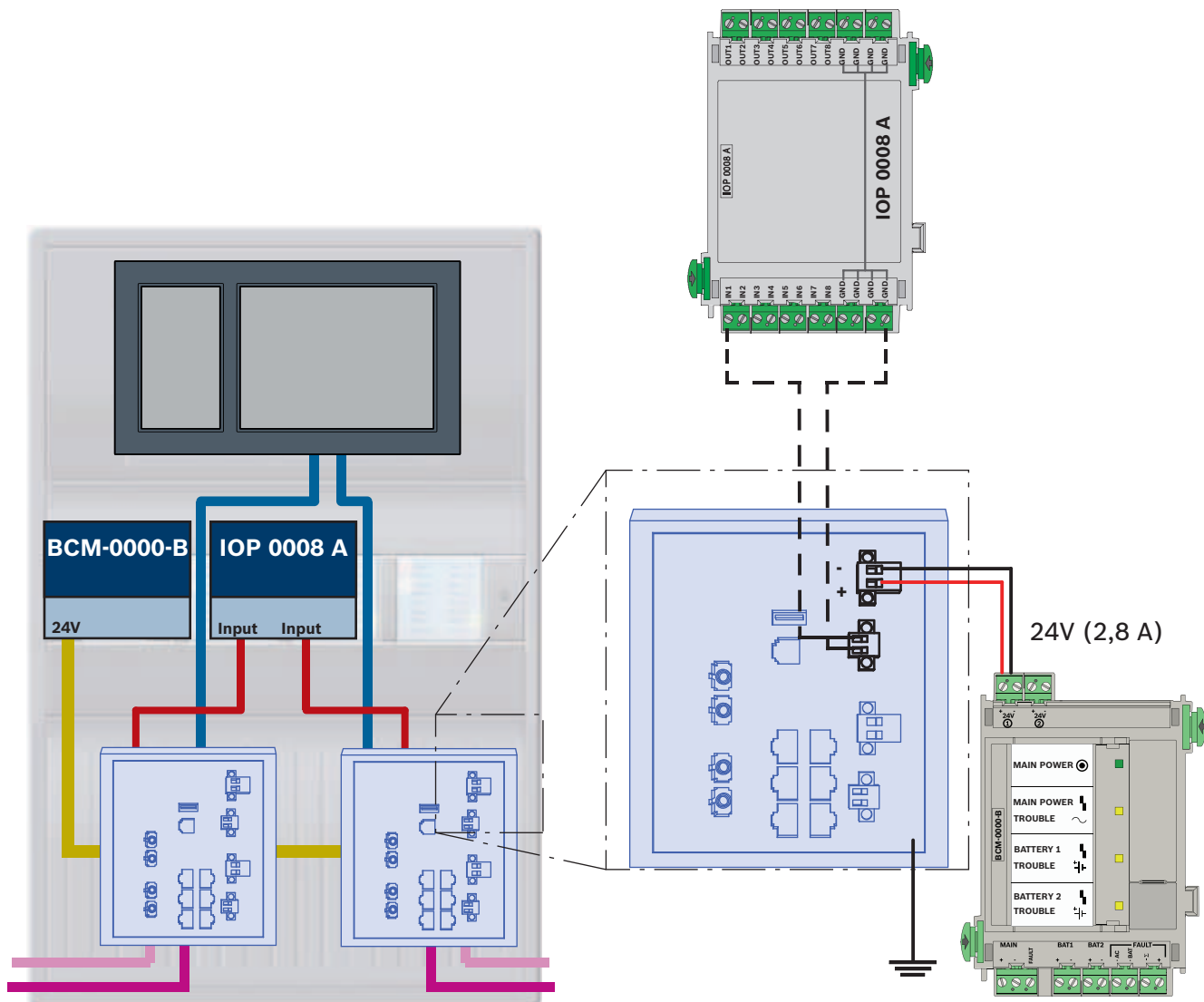
Wyjścia sygnału usterki switchów można podłączyć do wejść kontrolera centrali lub modułu wejścia i wyjścia IOP.





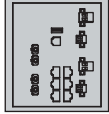


Uwaga!

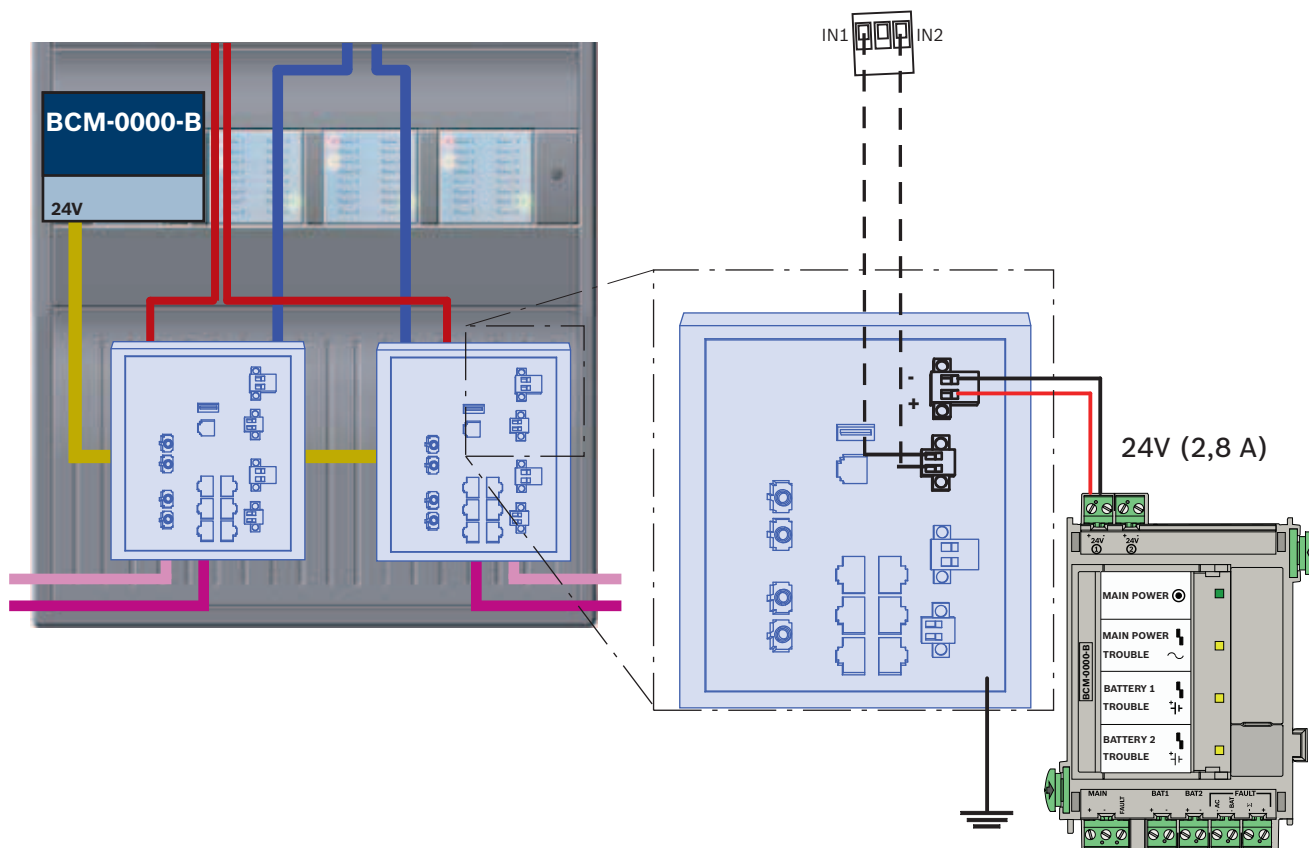
Podłączenie przekaźnika usterki jest wymagane tylko w przypadku zastosowań spełniających co najmniej jeden z poniższych warunków:
Istnieje połączenie pomiędzy 2 switchami. Jest to możliwe, np. w przypadku sieci szkieletowej z podpętlami.
Zasilanie przełącznika jest zaprojektowane nadmiarowo.

Podłączenie przeliczników z raportowaniem usterek do wejść modulu IOP:



Ikona	Opis
	Kabel TX Ethernet (miedziany)
	Kabel Ethernet FX (kabel światłowodowy)
	Zasilacz
	Transmisja usterki
	Przełącznik RSTP

Podłączanie przełączników z raportowaniem usterek do wejść kontrolera centrali



Ikona	Opis
	Kabel TX Ethernet (miedziany)
	Kabel Ethernet FX (kabel światłowodowy)
	Zasilacz
	Transmisja usterki
	Przełącznik RSTP



Uwaga!

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

13.3 Zdalna klawiatura

**Przeestroga!**

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

**Uwaga!**

Do podłączenia modułu zdalnej klawiatury do sieci central Ethernet należy używać wyłącznie konwerterów transmisji.

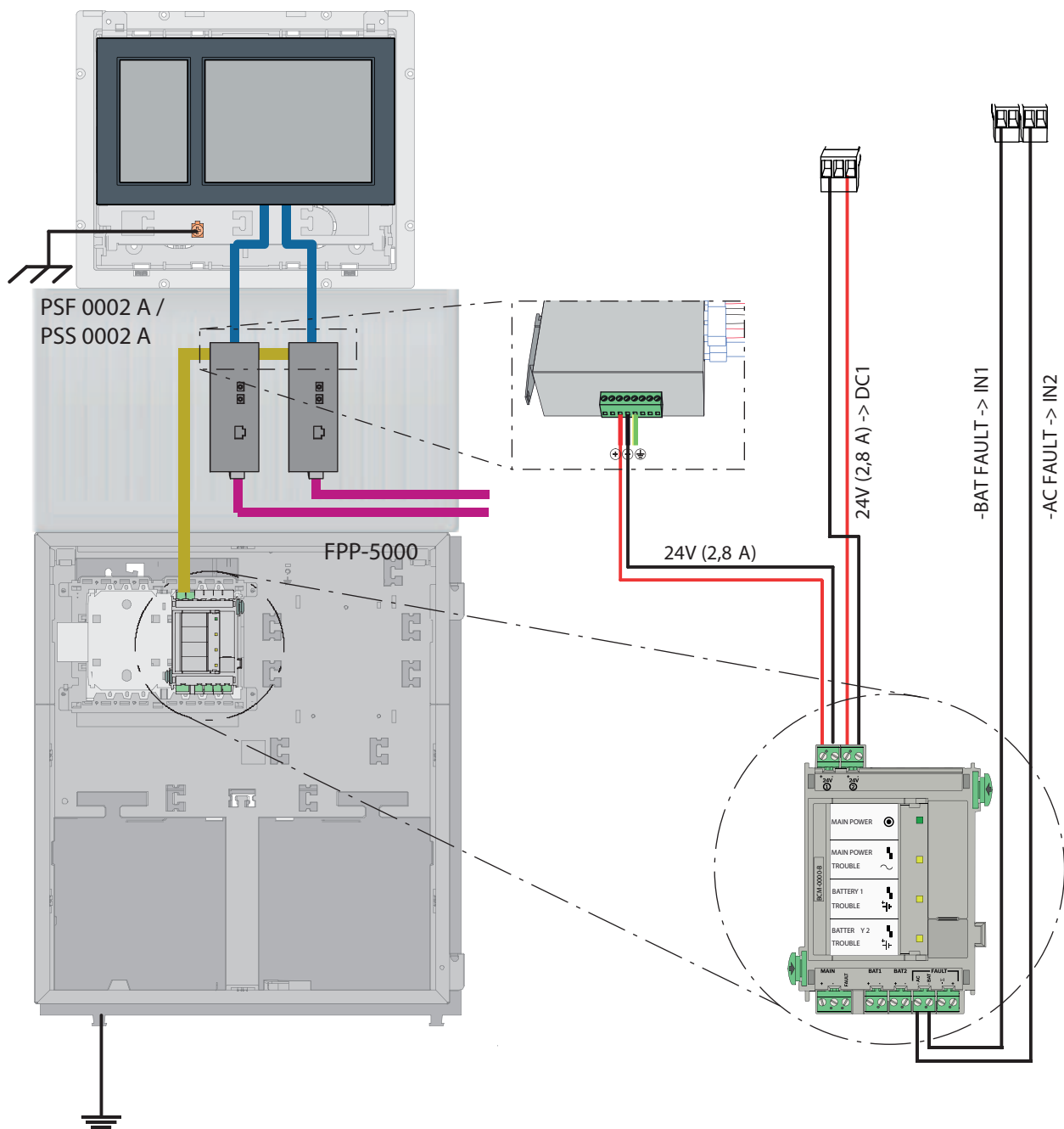
W przypadku zdalnej klawiatury niedozwolone jest użycie switchów.





Podłączenie do zdalnej klawiatury (zgodnej z VdS 2540)

Zewnętrzny zasilacz FPP-5000 jest używany do zasilania zdalnej klawiatury. Podłączenie do sieci jest tworzone przy użyciu dwóch konwerterów transmisji w PSS 0002 A lub USF 0000 A.

**Uwaga!**

Zewnętrzny zasilacz FPP-5000 i dodatkowa obudowa dla konwerterów mediów muszą być zamontowane na tej samej płaszczyźnie co zdalna klawiatura. Przewody zasilające zdalnej klawiatury i konwertera mediów nie są monitorowane pod kątem zwarcia narastającego i ciągłości, dlatego muszą być instalowane w obudowach montowanych na tej samej płaszczyźnie co obudowa zdalnej klawiatury.



Ikona	Opis
	Kabel TX Ethernet (miedziany)
	Kabel Ethernet FX (kabel światłowodowy)
	Zasilacz
	Konwerter transmisji

14 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 przetącznika podłączonego do sieci.

14.1 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 adres węzła fizycznego (**PNA/RSN**) w poszczególnych węzłach
- Dopasuj numery linii okablowania sieciowego, aby utworzyć planowaną topologię
- Sprawdź, czy wyświetlana topologia jest poprawna
- W razie potrzeby podłącz system zarządzania budynkiem, dźwiękowy system alarmowy, system integrujący i przetączniki
- 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

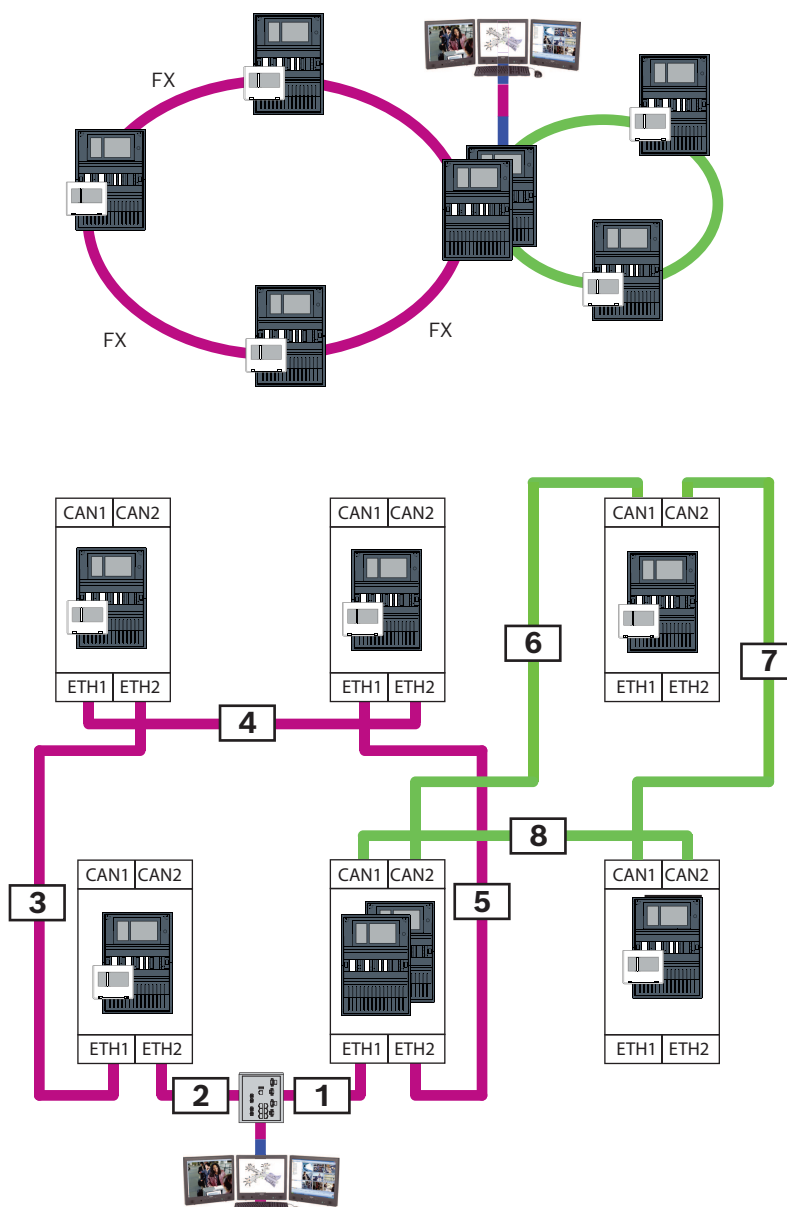
Po ponownym uruchomieniu sieci należy sprawdzić komunikaty o błędach i w razie potrzeby naprawić ewentualne błędy.

14.2 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 **Sieć** jako **Typ linii** w oknie **Interfejs sieciowy**, wtedy numerem linii musi być 0 dla wszystkich połączeń.



Rysunek 14.1: Przykład sieci i możliwe numerowanie linii

14.3 Przetłączniki

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

15 Załącznik

15.1 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	Ogólna usterka sieci	Niezgodna wersja oprogramowania sieciowego centrali. Istnieją 2 różne wersje oprogramowania.
Grupowanie usterek związanych z siecią			
135.0.6.1	Sieć 2.1	Zdublowany adres IP	Ares IP został przypisany dwa razy.
135.0.6.2	Sieć 2.2	Ustawienia IP	Konfiguracja IP raportującej centrali różni się od konfiguracji RPS.
135.0.6.3	Sieć 2.3	Ustawienia nadmiarowości	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	Awaryjny RSTP	Centrala raportująca przeszła z trybu RSTP do trybu STP (tryb zgodności). Urządzenie STP zostało podłączone do sieci.
135.0.7.2	Sieć 3.2	Zmiana topologii RSTP	Topologia sieci RSTP została zmieniona. Na przykład dodano inne urządzenie RSTP do sieci. Komunikat ten może być generowany w przypadku przerwania linii.
135.0.7.3	Sieć 3.3	Typ łącza RSTP - Point2Point	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	Usterka CAN 1	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	Usterka CAN 2	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	Usterka Ethernet 1	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	Usterka Ethernet 2	Transmisja danych do linii Ethernet 2 jest ograniczona. Możliwe przyczyny to m.in. uszkodzenia kabli, rozłączone kable, zakłócenia kablowe.

Indeks

A

adres MAC	19
Adres węzła fizycznego	14
Adresowanie	
Adres węzła fizycznego	14

B

Bezpieczna brama sieciowa	35, 36
---------------------------	--------

D

Dźwiękowy system alarmowy	45
---------------------------	----

E

Ethernet, ustawienia standardowe	15
----------------------------------	----

G

Górne limity	13
--------------	----

I

Interfejs CAN	56
Interfejs Ethernet	56
Interfejs RS232	56
Interfejs USB	56

K

Kontroler centrali	
System sieciowy	56

L

LLDP	20
------	----

P

Parametry	
RSTP	15
Parametry RSTP	15
PAVIRO	9, 45
Połączenie z siecią	
Długość kabla	25
Topologia pętli	25
Połączenie z siecią poprzez CAN	9
Połączenie z siecią poprzez TCP/IP	9
Praesideo	9, 45

R

Redundancja	
Adresowanie	14
Remote Alert	39
Remote Connect	35
Remote Maintenance	39, 40
dla sieci Private Secure Network	40
Remote Services	35
Podłącz bezpieczną bramę sieciową	36
Rozdzielanie podsieci	37
RSTP	20

S

sieci	
Limity	13
Sieć	
Adresowanie	59
Kabel	25
Kontroler centrali	56
Limity	13
Sieć CAN	9
Sieć Ethernet	9
Sieć: Okablowanie	25
System zarządzania budynkiem	9, 41, 56
System zarządzania budynkiem, Topologie	43, 44
Średnica sieci	20

T

Topologie	43, 44
Topologie CAN	11
Topologie sieci Ethernet	11
Topologie, CAN	11
Topologie, Ethernet	11
Topologie, z systemem zarządzania budynkiem	43, 44

U

Usługi	9
Usługi zdalne	
Aktywacja dzierżawy FSE	39
Łączenie z FSP-5000-RPS	39
Tworzenie dzierżawcy	38
Ustawienia standardowe, Ethernet	15

Bosch Sicherheitssysteme GmbH

Robert-Bosch-Platz 1

70839 Gerlingen

Niemcy

www.boschsecurity.com

© Bosch Sicherheitssysteme GmbH, 2025

Rozwiązania do budynków podnoszące jakość życia

202503251631