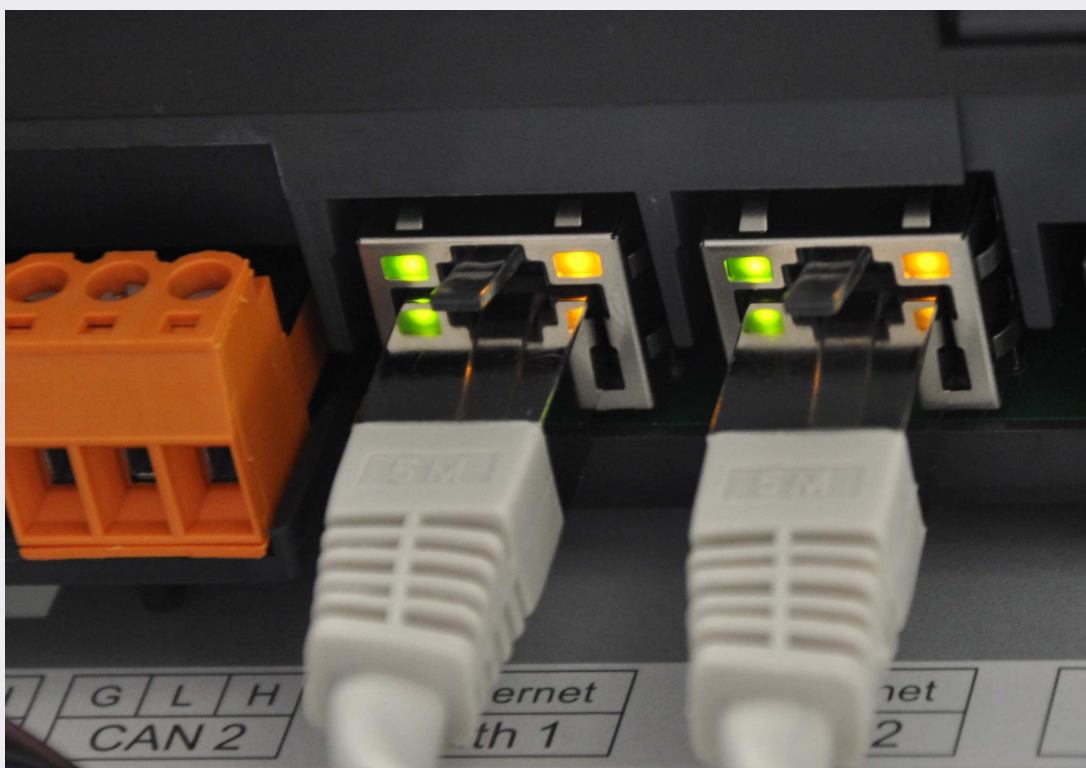




Modułowa centrala sygnalizacji pożaru

FPA-5000



BOSCH

pl

Networking Guide

Spis treści

1	Instrukcje bezpieczeństwa	5
2	Wstęp	6
3	Połączenie z siecią Ethernet	7
3.1	Procedura	7
3.1.1	Standardowa procedura dotycząca mniejszych projektów	7
3.1.2	Średnie i duże projekty	7
3.2	Informacje ogólne o sieci	8
3.2.1	Protokoły	8
3.2.2	Pojemność sieci	8
3.2.3	Stosowane kable	10
3.2.4	Rozbudowa istniejących sieci	11
3.2.5	Komunikacja Ethernet/IP	11
3.3	Topologie	12
3.3.1	Klucz	15
3.3.2	Pętla Ethernet	16
3.3.3	Pętla Ethernet z serwerem OPC	17
3.3.4	Pętla Ethernet z serwerem OPC do nadmiarowego kontrolera centrali	18
3.3.5	Podwójna pętla Ethernet/CAN	19
3.3.6	Sieć szkieletowa Ethernet z podpętlami (Ethernet/CAN)	20
3.3.7	Podłączanie pętli Ethernet	23
3.4	Sieci UGM-2040	24
3.5	Dźwiękowy system alarmowy w sieci IP	25
3.6	Remote Connect	25
3.7	Remote Maintenance	27
3.8	Remote Alert	30
4	Połączenie z magistralą CAN	31
4.1	Połączenie z dźwiękowym systemem alarmowym	33
4.2	Remote Connect	33
5	Remote Services krok po kroku	35
6	Ustawienia protokołu RPS	38
6.1	Węzły sieci	38
6.2	Numery linii	38
6.3	Przełączniki	39
6.4	Serwery OPC	39
6.5	Serwery UGM-2040	40
7	Instalacja	41
7.1	Instalacja konwerterów transmisji w ramie montażowej	41
7.2	Instalacja konwerterów transmisji w PSS 0002 A/USF 0000 A	42
7.3	Ustawienia konwertera transmisji	43
7.4	Instalowanie przełączników w PSS 0002 A/USF 0000 A	44
7.5	Ustawienia przełącznika	45
7.5.1	Przypisanie adresu IP	46
7.5.2	Programowanie ustawień nadmiarowości	47
7.5.3	Programowanie przekaźnika usterki	47
7.5.4	Programowanie monitoringu połączeń	48
7.5.5	Priorytet QoS, dotyczy tylko UGM-2040	48
7.5.6	Jak włączyć śledzenie IGMP	48
7.6	Sieć CAN	50

8	Połączenia	60
8.1	Okablowanie kontrolera centrali	60
8.1.1	Konwertery transmisji i zasilanie	60
8.2	Przełącznik z zasilaniem i przekaźnikiem usterki	61
8.3	Okablowanie modułu zdalnego sterowania FMR-5000	63
9	Załącznik	66
9.1	Komunikaty o błędzie w sieci Ethernet	66
	Indeks	67

1 Instrukcje bezpieczeństwa

**Uwaga!**

Konfiguracja ustawień sieciowych centrali sygnalizacji pożarowej wymaga osobnej sieci Ethernet.

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

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

**Uwaga!**

Aby zapewnić konfigurację sieciową zgodną z normą EN 54, należy korzystać wyłącznie z elementów zatwierdzonych do użytku w sieciach obsługujących centrale sygnalizacji pożarowej.

**Przestroga!**

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

**Przestroga!**

Usługa Remote Maintenance for Private Secure Network wymaga bezpiecznego połączenia IP. Z tego powodu w przypadku usługi Remote Maintenance for Private Secure Network dostępna jest sieć IP oparta na DSL z opcjonalnym bezprzewodowym dostępem po stronie centrali. Usługa Remote Maintenance for Private Secure Network jest dostępna tylko w Niemczech wraz z umową o świadczenie usług zawartą z firmą Bosch ST-IE.

**Uwaga!**

W przypadku zastosowań standardowych należy korzystać tylko ze standardowych ustawień sieciowych.

Zmiany standardowych ustawień sieciowych są dozwolone tylko w przypadku doświadczonych użytkowników dysponujących odpowiednią wiedzą na temat sieci.

**Niebezpieczeństwo!**

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. Fotodioda CLASS 2M, długość fali 650 nm, wyjście < 2 mW (zgodnie z normą DIN EN 60825-1:2003-10).

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 sieciowych.

Niniejsza instrukcja połączeń sieciowych zawiera omówienie ramowych 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 centrali MPC-xxxx-C znajduje się w podręczniku użytkownika dołączonym do urządzenia.

Interfejs użytkownika aplikacji do programowania FSP-5000-RPS został opisany w pomocy online.



Uwaga!

Drogi Kliencie,

dokładamy wszelkich starań, aby nasza dokumentacja była jak najlepsza. Jeśli masz jakieś sugestie lub chcesz wskazać ewentualne błędy, możesz wysłać odpowiednią wiadomość na adres: ST.TechComFire@de.bosch.com.

3 Połączenie z siecią Ethernet

3.1 Procedura

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

3.1.1 Standardowa procedura dotycząca mniejszych projektów

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 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 sieć.
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.
8. Wykonaj resetowanie, aby wyzerować oczekujące komunikaty o błędach. Napraw błędy.

Upřednie skonfigurowanie ustawień sieciowych w centralach sygnalizacji pożaru ma tę zaletę, że umożliwia zaprogramowania wszystkich pozostałych central za pośrednictwem jednej centrali.

3.1.2 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 RPS.
8. Upewnij się, że każda centrala działa prawidłowo.
9. Uruchom poszczególne pętle sieci jedną po drugiej, zgodnie z topologią.
Uruchom sieć szkieletową.
 - Utwórz konfigurację dotyczącą sieci szkieletowej w RPS. 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.

3.2 Informacje ogólne o sieci

W sieci połączenia Ethernet są monitorowane w sposób ciągły. W przypadku zerwania połączenia wykrywana jest przerwa. Wykrywane są również naprawione połączenia.

Adresy MAC

Każdy kontroler centrali ma trzy adresy MAC.

- Adres MAC hosta
- Adres MAC połączenia sieciowego 1 (Eth 1)
- Adres MAC połączenia sieciowego 2 (Eth 2)

Diagnostyka sieci danej centrali zawsze pokazuje adresy MAC hostów połączonych za pośrednictwem sieci.

3.2.1 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!

Hasło SNMP w sieci to PUBLIC.

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 ponownie zaraz po usunięciu awarii.

3.2.2 Pojemność sieci

Pojemność sieci FPA-RSTP Ethernet nie może być większa niż 32.

Definicja

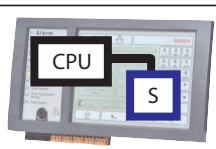
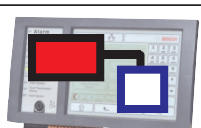
Pojemność sieci odpowiada liczbie przełączników RSTP na najdłuższym możliwym odcinku bez pętli pomiędzy dowolnymi dwoma końcowymi punktami sieci.

Należy wziąć pod uwagę następujące kwestie dotyczące sieci FPA-RSTP Ethernet:

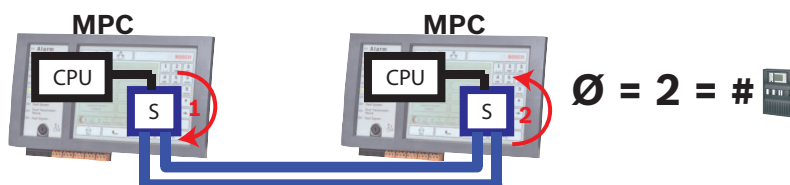
- Każdy MPC zawiera punkt końcowy i wewnętrzny przełącznik RSTP.
- Kombinacja MPC i redundantnego MPC liczy się jako jeden przełącznik RSTP.
- Konwertery transmisji nie są traktowane jako przełączniki RSTP.

- Najdłuższy możliwy odcinek nie może obejmować połączeń CAN.
- Pojemność nie uwzględnia serwerów OPC.

Klucz

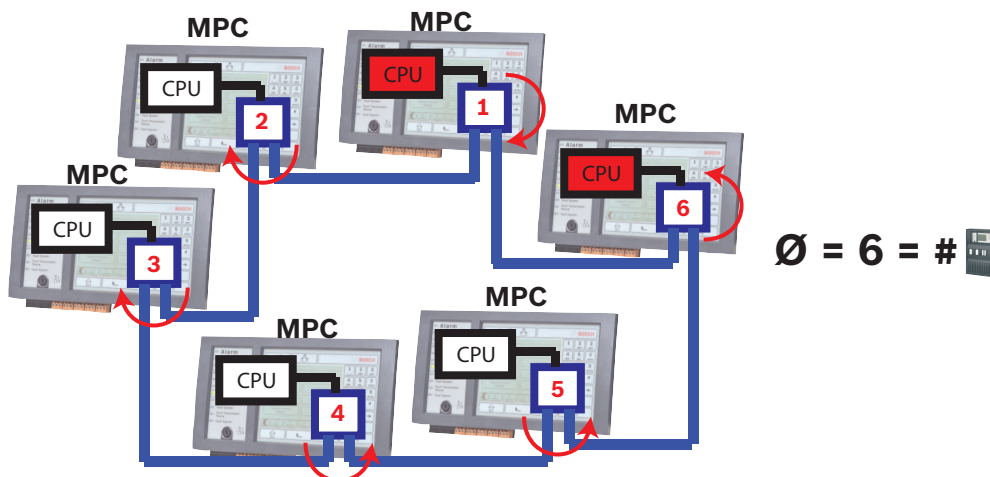
	Procesor główny w kontrolerze centrali lub w zdalnej klawiaturze.
	Wewnętrzny przełącznik RSTP w kontrolerze centrali lub w zdalnej klawiaturze.
	Kontroler centrali lub zdalna klawiatura z procesorem głównym i wewnętrznym przełącznikiem RSTP.
	Nadmiarowy kontroler centrali z procesorem głównym i wewnętrznym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

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



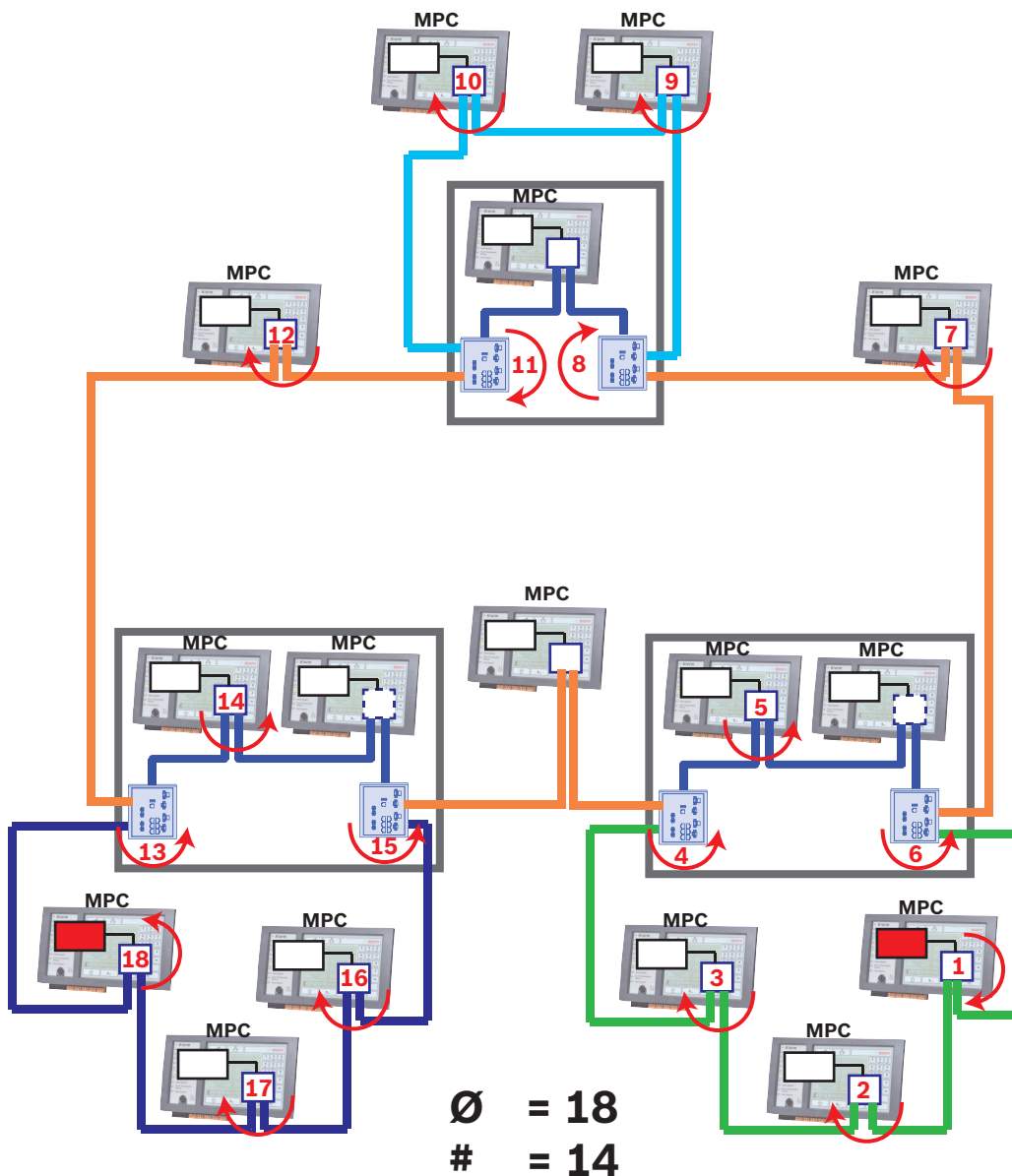
Rysunek 3.1: Pojemność sieci pętli z 2 centralami

W pętli central bez zewnętrznych przełączników pojemność sieci odpowiada liczbie zainstalowanych central.



Rysunek 3.2: Pojemność sieci pętli z 6 centralami

Jeśli sieć szkieletowa i podpętla są połączone ze sobą za pośrednictwem przełączników RSTP, które nie są wbudowane w kontroler centrali, należy również uwzględnić przełączniki RSTP.



Rysunek 3.3: Pojemność sieci szkieletowej z podpętlami

Na rysunku pokazano, że określenie pojemności zawsze wymaga znalezienia najdłuższej ścieżki.

3.2.3

Stosowane kable

Instalacje sieciowe wymagają korzystania wyłącznie z następujących kabli:

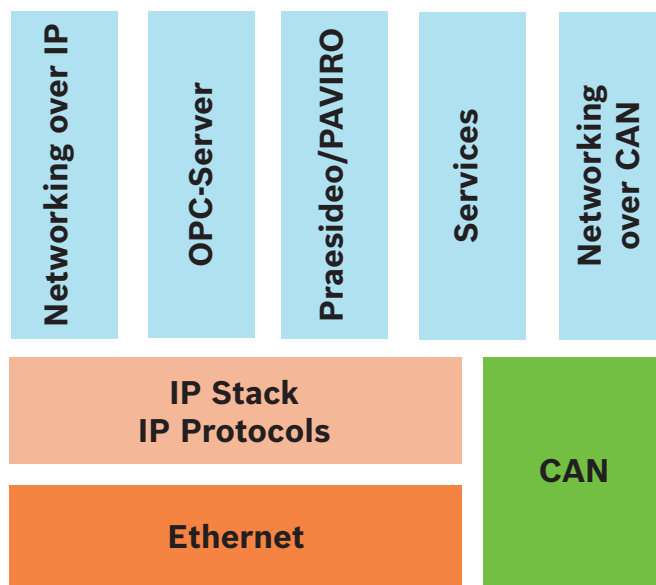
- Kabel Ethernet
Kabel sieciowy Ethernet, ekranowany, CAT5e lub lepszy.
Należy pamiętać o minimalnym promieniu zgięcia określonym w specyfikacji kabla.
- Kabel światłowodowy
Tryb multi-mode: sieciowy kabel światłowodowy Ethernet, duplex I-VH2G 50/125μ lub duplex I-VH2G 62.5/125μ, wtyczka SC.
Tryb pojedynczy: sieciowy kabel światłowodowy Ethernet, duplex I-VH2E 9/125μ, wtyczka SC.

Należy pamiętać o minimalnym promieniu zgięcia określonym w specyfikacji kabla.

3.2.4 Rozbudowa istniejących sieci

Aby zapewnić niezawodną komunikację pomiędzy różnymi wersjami central (np. MPC, wersja B), wszystkie centrale muszą mieć tę samą wersję oprogramowania sprzętowego.

3.2.5 Komunikacja Ethernet/IP



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

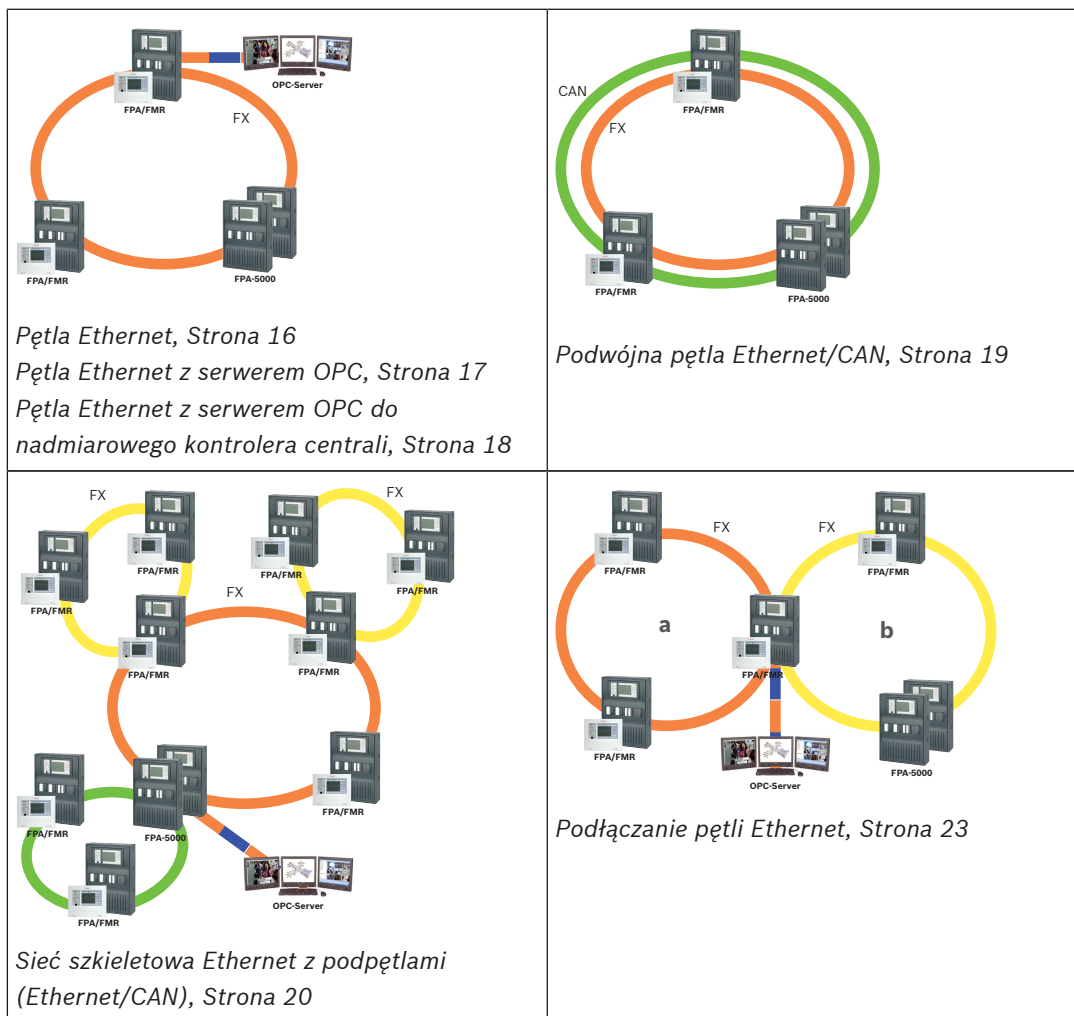
- połączenie z siecią poprzez TCP/IP
W FSP-5000-RPS włącz komunikację między centralami w sieci Ethernet
- Serwery OPC
Dodaj serwer OPC do konfiguracji FSP-5000-RPS.
- Połączenie z systemem Praesideo/PAVIRO
Dodaj dźwiękowy system alarmowy do konfiguracji FSP-5000-RPS i skonfiguruj wyzwalacze wirtualne.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

Jeśli interfejs Ethernet kontrolera centrali ma służyć jedynie do komunikacji z serwerem OPC lub usługami Remote Services, wyłącz połączenie centrali z siecią poprzez TCP/IP. W przeciwnym razie dane 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.

3.3

Topologie

Możliwe są następujące topologie:



Poniższe ustawienia, uwagi i ograniczenia dotyczą wszystkich topologii:



Uwaga!

Zgodnie z normą EN 54-2, dla każdej centrali można podłączyć maksymalnie 512 punktów detekcji.

W przypadku przekroczenia tej liczby centrala musi być zaprojektowana nadmiarowo. Ze względów technicznych maksymalna liczba punktów detekcji, które można podłączyć, to 2048.



Uwaga!

W przypadku gdy centrala działa jako interfejs z podpętlą CAN, również musi być zaprojektowana nadmiarowo (zgodnie z normą EN 54-2), jeśli w podpętli podłączono więcej niż 512 punktów detekcji.

Ograniczenie to nie dotyczy pętli Ethernet, ponieważ przełączniki służące do połączenia dwóch pętli obsługują nadmiarowość.

**Uwaga!**

Używana sieć musi spełniać następujące wymagania minimalne:
Minimalna przepustowość: 1 Mb/s
Maksymalne opóźnienie: 250 ms

**Uwaga!**

Wymagania normy EN 54-13 dotyczące torów transmisji danych mogą być spełnione tylko w przypadku zastosowania kabli światłowodowych do połączeń Ethernet.
Połączenia w obudowach można wykonać za pomocą kabli Ethernet.

**Uwaga!**

Przełączniki i konwertery transmisji w sieciach Ethernet należy instalować w obudowach central. Instalacja na zewnątrz obudowy centrali jest niezgodna z normą EN 54.

**Uwaga!**

Aby zapewnić konfigurację sieciową zgodną z normą EN 54, należy korzystać wyłącznie z elementów zatwierdzonych do użytku w sieciach obsługujących centrale sygnalizacji pożarowej.

**Uwaga!**

Sieci obejmujące ponad 20 przełączników RSTP lub o pojemności większej niż 20 wymagają specjalnych ustawień.
Standardowe ustawienie w konfiguracji IP jest przeznaczone wyłącznie dla sieci z maksymalną liczbą 20 przełączników RSTP lub o maksymalnej średnicy 20.

Upewnij się, że RSN przypisany do centrali pasuje do RSN określonego w aplikacji do obsługi programowania. Odpowiada on za ustawienie ostatniego numeru adresu IP w ustawieniach standardowych.

Aktywuj opcję RSTP jako protokół nadmiarowości i dopasuj domyślne wartości standardowe.

Standardowe ustawienia Ethernet dotyczące FPA

W standardowych ustawieniach FPA aplikacja do programowania FSP-5000-RPS oraz moduł sterujący przyjmują ustawienie RSN takie jak ostatnia cyfra w adresie IP.

**Uwaga!**

Poprawne ustawienie RSN w kontrolerach centrali i aplikacji do programowania FSP-5000-RPS jest koniecznym warunkiem działania sieci.

**Uwaga!**

Użycie nadmiarowości 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 RSN 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)
- Parametry RSTP (ustawienia nadmiarowości)
 - Bridge Priority 32768
 - Hello Time 2
 - Max. Age 20
 - Forward Delay 15

**Uwaga!**

Ustawienia standardowe konfiguracji IP można stosować w sieciach obejmujących maksymalnie 20 przełączników RSTP.

W przypadku sieci z większą niż 20 liczbą przełączników RSTP wymagane są dodatkowe ustawienia odpowiadające topologii. Potrzebna jest do tego dogłębna znajomość zagadnień sieciowych.

Ustawienia pętli obejmujących więcej niż 20 przełączników RSTP

Jeśli sieć obejmuje ponad 20 przełączników RSTP, konieczne jest dopasowanie ustawień RSTP w kontrolerze centrali i aplikacji do programowania. Potrzebna jest do tego dogłębna znajomość zagadnień sieciowych. Kontrolery centrali są traktowane jak przełączniki RSTP. Nadmiarowe kontrolery centrali nie są traktowane jak przełączniki RSTP, ponieważ znajdujący się w nich przełącznik nie działa jako przełącznik RSTP.

Parametry

- W pętli można wykorzystać maksymalnie 32 węzły.
- Pojemność sieci nie może być większa niż 32, patrz *Pojemność sieci*, Strona 8.
- Sekcje transmisji Ethernet na zewnątrz obudowy centrali muszą być zaprojektowane jako połączenia kablem światłowodowym.
- Przełączniki nie mogą być używane na zewnątrz obudów central.
- Konwertery transmisji nie mogą być używane na zewnątrz obudów central.
- W przypadku FPA-1200 można wykorzystać w sieci tylko jedną centralę i trzy FMR-5000.

Charakterystyka

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

Informacje dodatkowe na temat użycia serwera OPC

Jeśli w sieci używane są serwery OPC, należy je dodać do aplikacji do programowania RPS. W oprogramowaniu RPS i na serwerze OPC muszą być skonfigurowane następujące ustawienia:

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

Standardowo serwer OPC używa portu 25000.

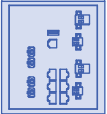
**Uwaga!**

Aplikacja do programowania FSP-5000-RPS:

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

3.3.1

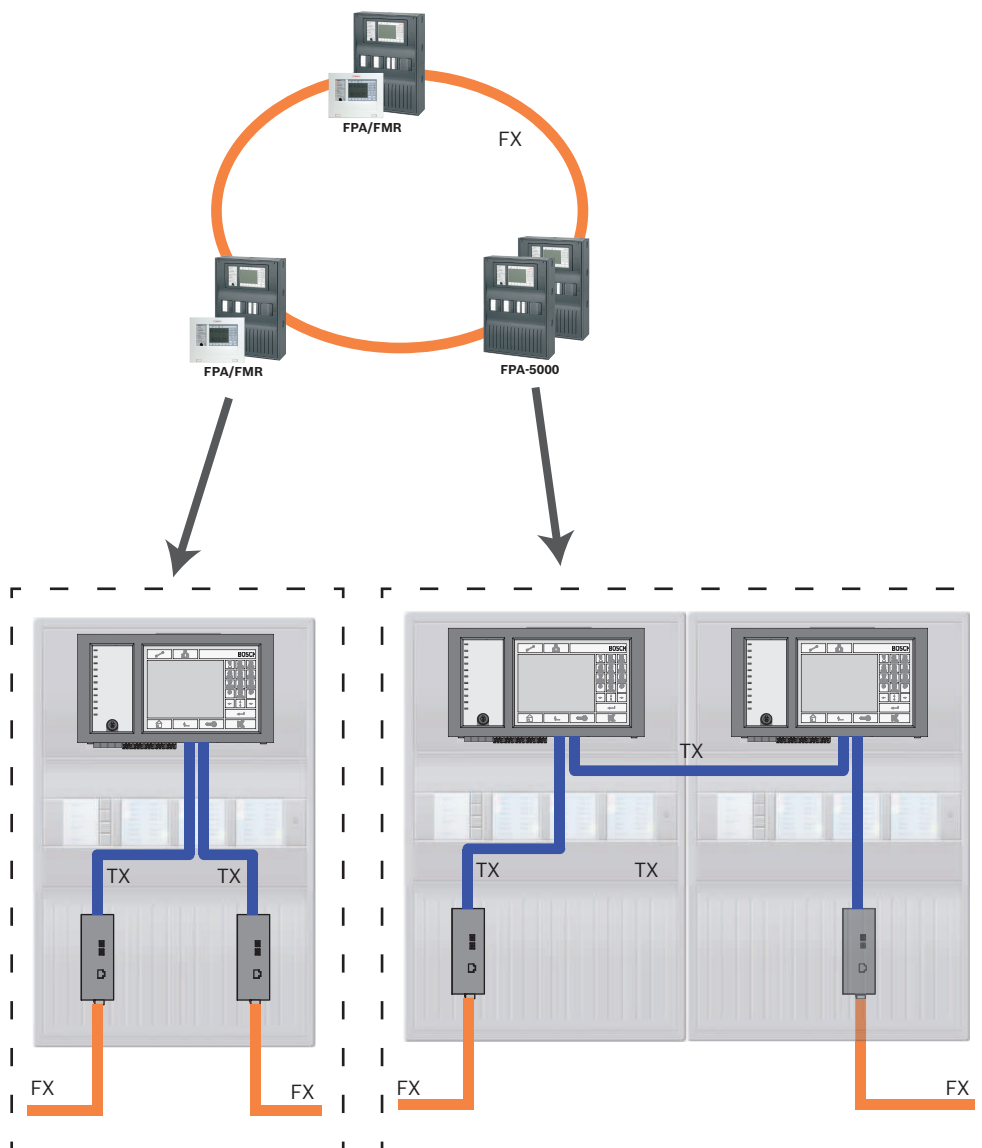
Klucz

Ikona	Opis
	Kabel Ethernet TX (miedziany)
	Kabel Ethernet FX (kabel światłowodowy)
	Kabel Ethernet TX lub FX
	Magistrala CAN
	Obudowa
 FPA/FMR	Centrala/zdalna klawiatura
 FPA-5000	Centrala nadmiarowa
	Przełącznik Ethernet Switch (zasadniczo Ethernet Switch MM)
	Konwerter transmisji
	Secure Network Gateway

3.3.2

Pętla Ethernet

Uwagi, opisy ustawień, parametrów i funkcji dotyczące tej konfiguracji znajdują się w części *Topologie, Strona 12*.



Rysunek 3.4: Pętla Ethernet

Klucz, patrz *Klucz, Strona 15*

3.3.3

Pętla Ethernet z serwerem OPC

Uwagi, opisy ustawień, parametrów i funkcji dotyczące tej konfiguracji znajdują się w części *Topologie, Strona 12*.

Więcej informacji zawiera część *Topologie, Strona 12*.

Przełącznik do podłączania serwera OPC musi być zaprogramowany oddzielnie.

Aby uzyskać informacje o programowaniu ustawień adresu IP i nadmiarowości przełącznika, patrz *Ustawienia przełącznika, Strona 45*. Ze względu na to, że przełącznik jest instalowany w bezpośrednim sąsiedztwie (bez wolnej przestrzeni), nie jest konieczne projektowanie nadmiarowego zasilania. Dlatego też wyjścia sygnału awarii nie są używane.

Należy upewnić się, że ustawienia RSTP w kontrolerach centrali, aplikacji do programowania RPS i przełączniku są identyczne.

Serwer OPC musi być zaprogramowany oddzielnie.

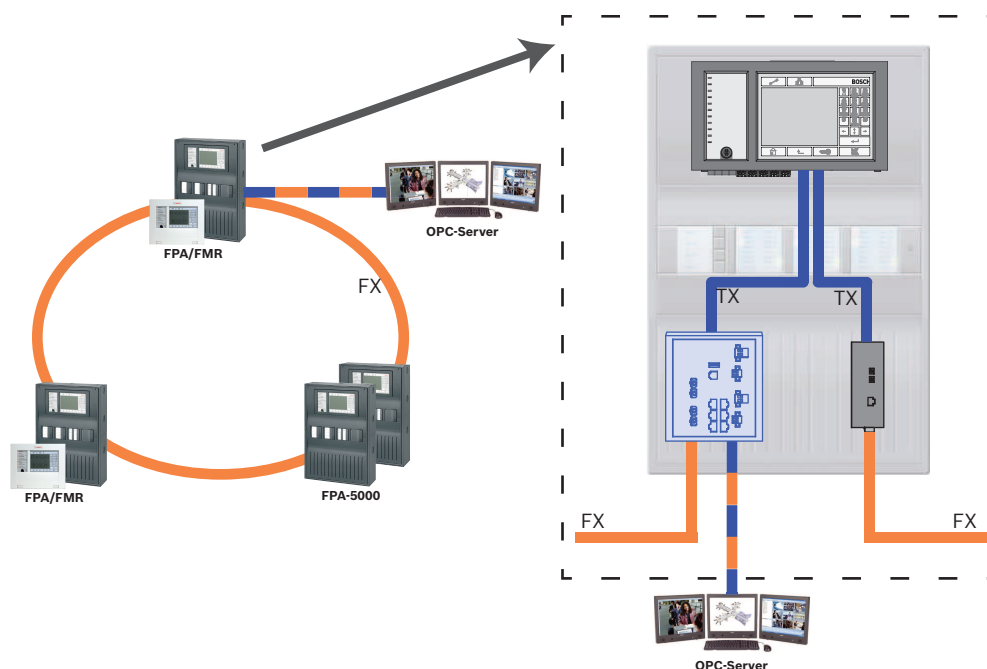
Aby uzyskać informacje o programowaniu adresu IP, węzłów sieci, grupy sieciowej i RSN, patrz *Serwery OPC, Strona 39*.

Standardowo serwer OPC używa portu 25000.

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

Parametry

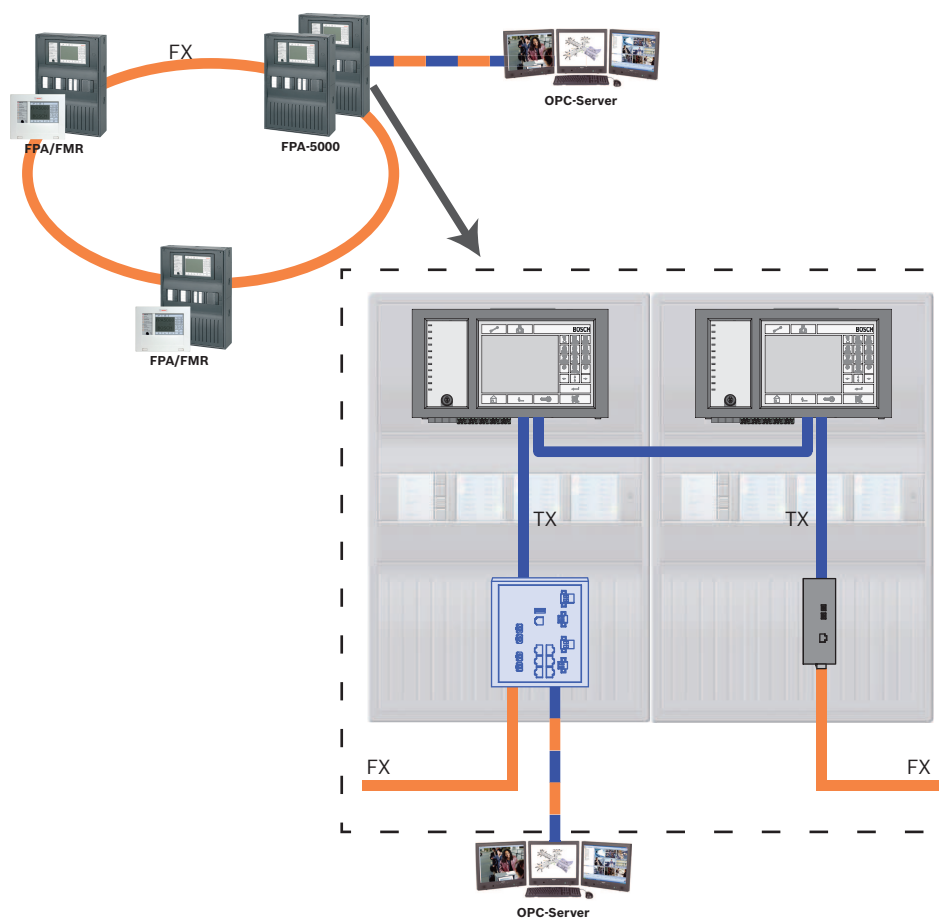
- Serwer OPC może być podłączony za pośrednictwem kabla Ethernet (miedzianego) lub kabla światłowodowego.



Rysunek 3.5: Pętla Ethernet z serwerem OPC

Klucz, patrz *Klucz, Strona 15*

3.3.4 Pętla Ethernet z serwerem OPC do nadmiarowego kontrolera centrali



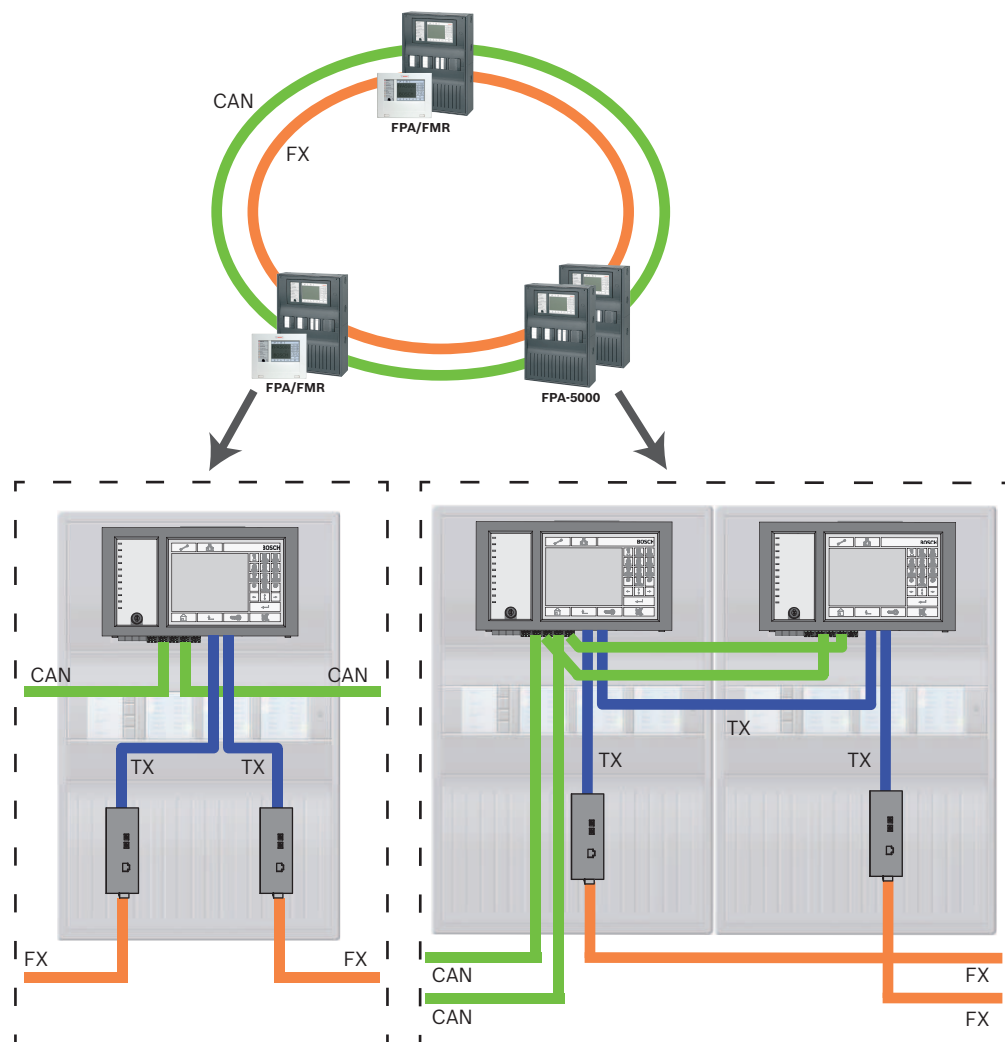
Rysunek 3.6: Pętla Ethernet z serwerem OPC do centrali nadmiarowej

Klucz, patrz *Klucz*, Strona 15

3.3.5

Podwójna pętla Ethernet/CAN

Uwagi, opisy ustawień, parametrów i funkcji dotyczące tej konfiguracji znajdują się w części *Topologie, Strona 12*.



Rysunek 3.7: Podwójna pętla Ethernet i CAN

Klucz, patrz *Klucz, Strona 15*

3.3.6

Sieć szkieletowa Ethernet z podpętlami (Ethernet/CAN)

Uwagi, opisy ustawień, parametrów i funkcji dotyczące tej konfiguracji znajdują się w części *Topologie, Strona 12*.

Więcej informacji zawiera część *Topologie, Strona 12*.



Uwaga!

Niniejsza topologia wymaga dodatkowej konfiguracji ustawień dla wszystkich węzłów RSTP w sieci szkieletowej. Potrzebna jest do tego dogłębna znajomość zagadnień sieciowych.

Należy pamiętać, że ta topologia wymaga określenia pojemności sieci (patrz *Pojemność sieci, Strona 8*). Tylko urządzenia RSTP są uwzględniane w pojemności sieci, połączone w sieć centrale CAN nie są uwzględniane.



Uwaga!

W przypadku gdy centrala działa jako interfejs z podpętlą CAN, również musi być zaprojektowana nadmiarowo (zgodnie z normą EN 54-2), jeśli w podpętli podłączono więcej niż 512 punktów detekcji.

Ograniczenie to nie dotyczy pętli Ethernet, ponieważ przełączniki służące do połączenia dwóch pętli obsługują nadmiarowość.

Ustawienia dodatkowe

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



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 pętle są częścią sieci szkieletowej!

Należy używać priorytetu RSTP 16384 w sieci szkieletowej.



Uwaga!

Im niższa jest wartość ustawienia, tym wyższy priorytet RSTP.

Ustawienia pętli obejmujących więcej niż 20 urządzeń RSTP

Kontrolery centrali połączone za pośrednictwem CAN nie są traktowane jako przełączniki RSTP podczas określania pojemności sieci.

Przełączniki do podłączenia serwera OPC i podpętli muszą być zaprogramowane oddzielnie.

Aby uzyskać informacje o programowaniu ustawień adresu IP i nadmiarowości przełączników, patrz *Ustawienia przełącznika, Strona 45*. W przypadku tej topologii użycie wyjść sygnału usterki przełącznika jest konieczne, jeśli zaprojektowano nadmiarowe zasilanie przełącznika lub istnieje połączenie typu przełącznik-przełącznik (patrz *Przełącznik z zasilaniem i przekaźnikiem usterki, Strona 61*).

Należy upewnić się, że ustawienia RSTP w kontrolerach centrali, aplikacji do programowania RPS i przełączniku są identyczne.

**Uwaga!**

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

Serwer OPC musi być zaprogramowany oddzielnie.

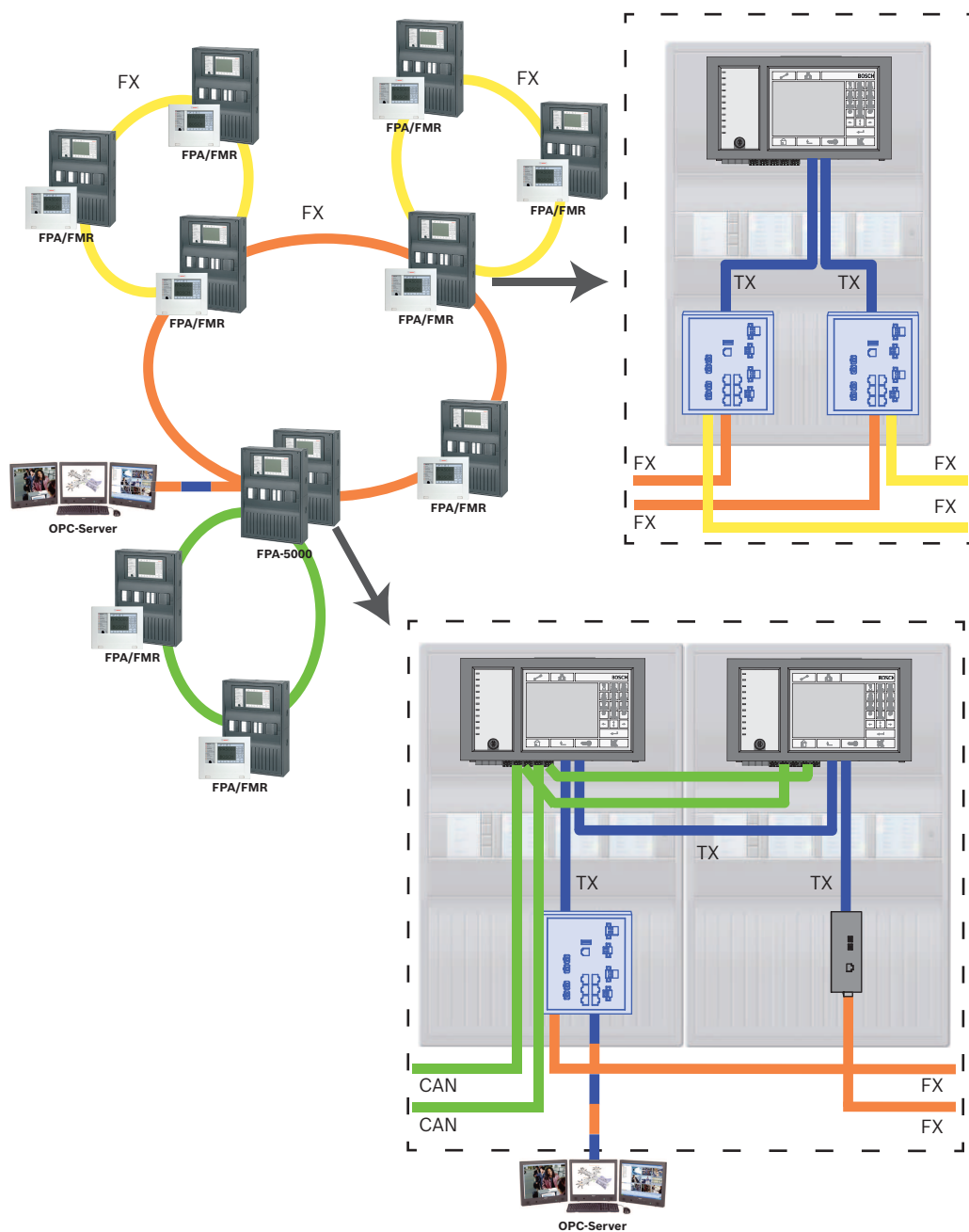
Aby uzyskać informacje o programowaniu adresu IP, węzłów sieci, grupy sieciowej i RSN, patrz *Serwery OPC, Strona 39*.

Standardowo serwer OPC używa portu 25000.

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

Parametry

- Serwer OPC może być podłączony za pośrednictwem kabla Ethernet lub kabla światłowodowego.



Rysunek 3.8: Sieć szkieletowa Ethernet z podpętlami

Klucz, patrz *Klucz*, Strona 15

3.3.7

Podłączanie pętli Ethernet

Uwagi, opisy ustawień, parametrów i funkcji dotyczące tej konfiguracji znajdują się w części *Topologie, Strona 12*.

Więcej informacji zawiera część *Topologie, Strona 12*.

**Uwaga!**

Niniejsza topologia wymaga dodatkowej konfiguracji ustawień dla wszystkich węzłów 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), Strona 20*). 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!

Należy używać priorytetu RSTP 16384 w sieci szkieletowej.

**Uwaga!**

Im niższa jest wartość ustawienia, tym wyższy priorytet RSTP.

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

Aby uzyskać informacje o programowaniu ustawień adresu IP i nadmiarowości przełącznika, patrz *Ustawienia przełącznika, Strona 45*. W przypadku tej topologii użycie wyjść sygnału usterki przełącznika jest konieczne, jeśli zaprojektowano nadmiarowe zasilanie przełącznika lub istnieje połączenie typu przełącznik-przełącznik. Aby uzyskać informacje o połączeniach, patrz *Przełącznik z zasilaniem i przekaźnikiem usterki, Strona 61*.

Należy upewnić się, że ustawienia RSTP w kontrolerach centrali, aplikacji do programowania RPS i przełączniku są identyczne.

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

Serwer OPC musi być zaprogramowany oddzielnie.

Aby uzyskać informacje o programowaniu adresu IP, węzłów sieci, grupy sieciowej i RSN, patrz *Serwery OPC, Strona 39*.

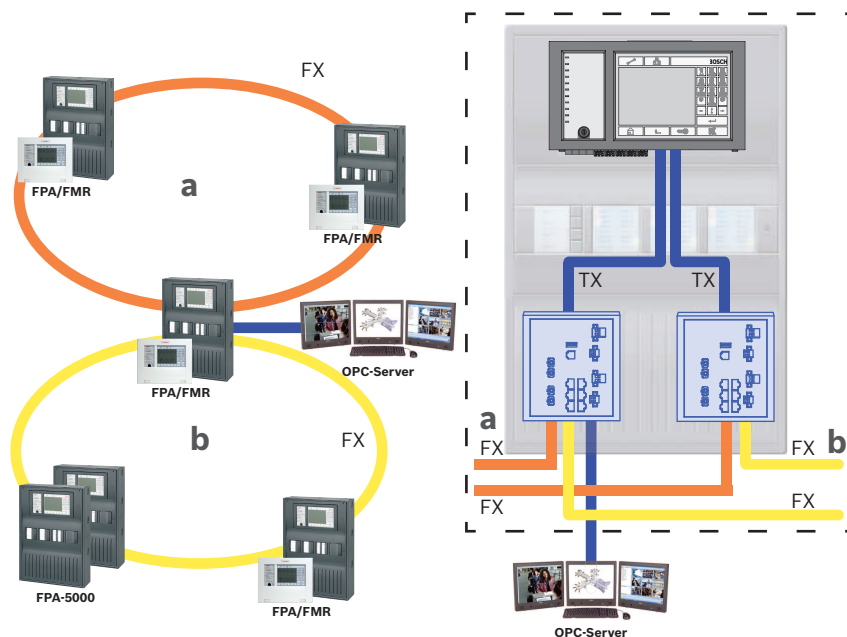
Standardowo serwer OPC używa portu 25000.

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

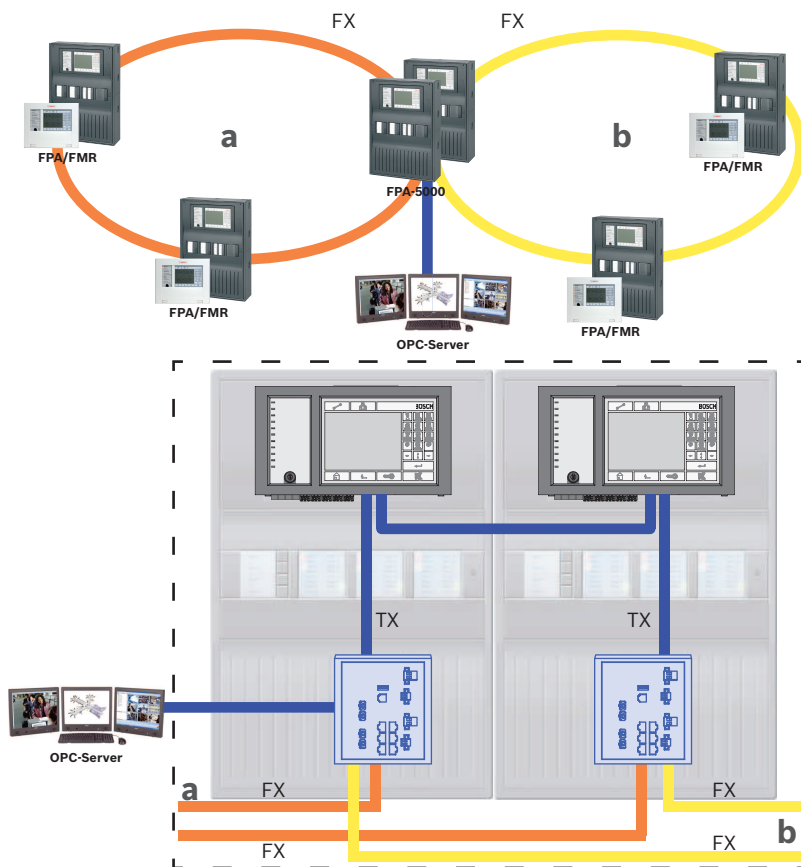
Parametry

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

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



Rysunek 3.9: Podłączanie pętli Ethernet za pośrednictwem centrali nienadmiarowej



Rysunek 3.10: Podłączanie pętli Ethernet za pośrednictwem centrali nadmiarowej

Klucz, patrz *Klucz*, Strona 15

3.4

Sieci UGM-2040

Topologie do zainstalowania i ustawienia sieciowe do zaprogramowania można uzyskać za pomocą narzędzia planistycznego UGM 2040 BMA. Patrz także UGM 2040 BMA Anschaltehandbuch.

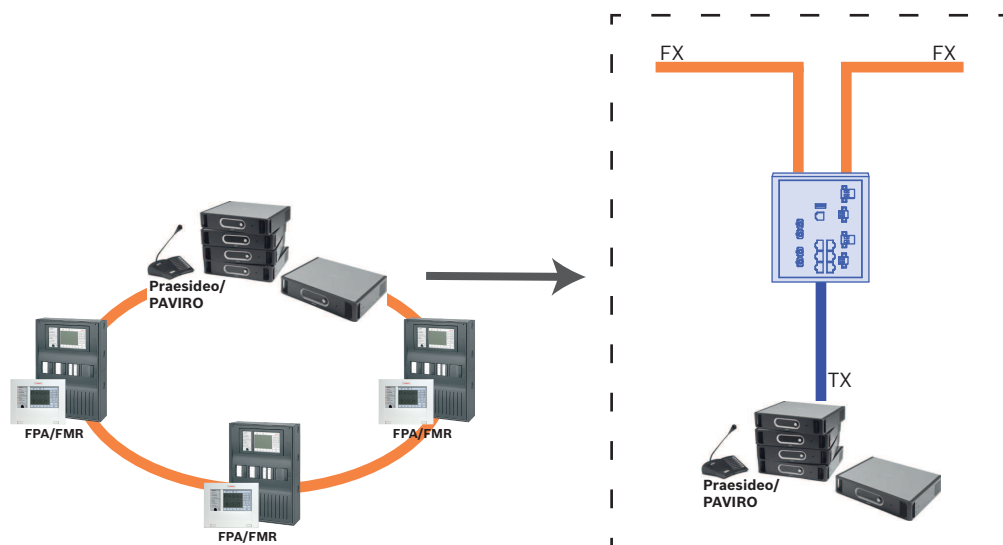
3.5 Dźwiękowy system alarmowy w sieci IP



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).

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



Rysunek 3.11: Pętla Ethernet z Praesideo/PAVIRO

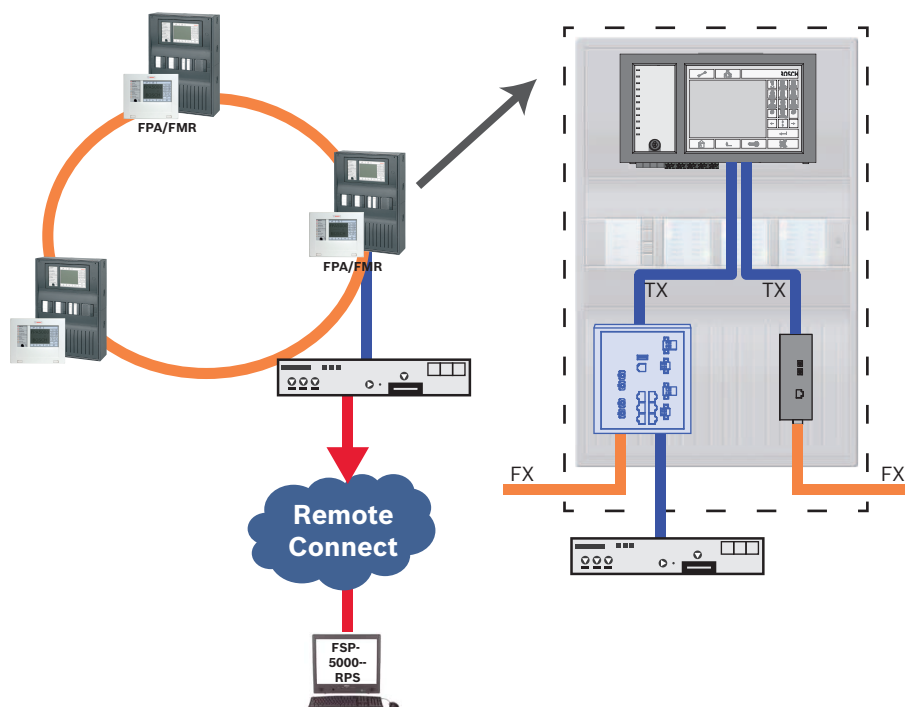
Należy użyć przełącznika Ethernet Switch (zasadniczo Ethernet Switch MM BPA-ESWEX-RSR20) przeznaczonego do obsługi oprogramowania sprzętowego centrali w wersji 2.8. Aby uniemożliwić przesyłanie ruchu multemisji zgodnego z normą EN 54-2 do systemu Praesideo/PAVIRO, należy aktywować śledzenie IGMP w przełączniku Ethernet Switch MM (patrz *Jak włączyć śledzenie IGMP*, Strona 48).

3.6 Remote Connect

Usługa Remote Connect zapewnia bezpieczne połączenie internetowe, które umożliwia zdalny dostęp do centrali. W przypadku usługi Remote Connect należy skorzystać z bezpiecznej bramy sieciowej Secure Network Gateway (CTN: C1500).

W przypadku sieci centrali jedna z centrali w sieci musi być podłączona do bezpiecznej bramy sieciowej Secure Network Gateway. To połączenie powinno być dedykowanym połączeniem Ethernet. Usługa Remote Connect musi być włączona w konfiguracji FSP-5000-RPS tej centrali.

Poniższa topologia przedstawia połączenie kontrolerów centrali w sieci Ethernet, gdzie bezpieczna brama sieciowa Secure Network Gateway jest podłączona do sieci za pośrednictwem przełącznika Ethernet Switch (zasadniczo Ethernet Switch MM).



Rysunek 3.12: Usługa Remote Connect w pętli Ethernet



Uwaga!

Do połączenia centrali za pośrednictwem FX można używać tylko konwerterów transmisji.

Aby uniemożliwić przesyłanie ruchu multimedialnego zgodnego z normą EN 54-2 do routera, należy użyć przełącznika Ethernet Switch (zasadniczo Ethernet Switch MM BPA-ESWEX-RSR20) przeznaczonego do obsługi centrali w wersji 2.8. Należy aktywować śledzenie IGMP w przełączniku Ethernet Switch (patrz *Jak włączyć śledzenie IGMP*, Strona 48).

**Uwaga!**

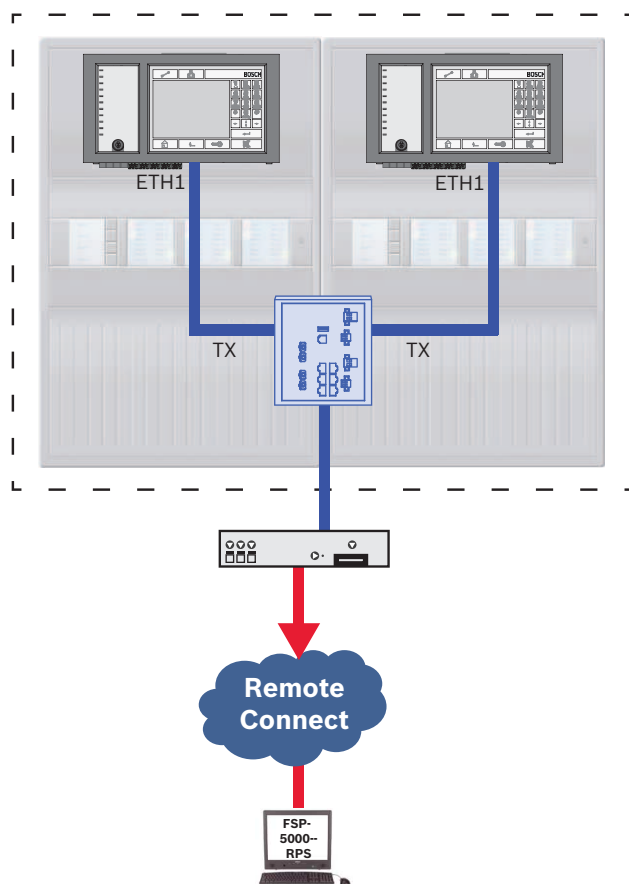
Router internetowy (lub sieć firmowa zapewniająca dostęp do Internetu), a także Secure Network Gateway muszą być oddzielone podsieciami. Centrale sieciowe nie mogą znajdować się w jednej podsieci z routerem internetowym. Nie jest również możliwe nakładanie się na siebie podsieci.

Jeśli podsieci się na siebie nakładają, trzeba je oddzielić, zmieniając adresy IP po stronie sieci centrali. Oprócz tego trzeba zastosować zmiany w Secure Network Gateway. 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 **Brama domyślna**: w konfiguracji kontrolera centrali musi być zgodny z adresem IP Secure Network Gateway.

Aby podłączyć Secure Network Gateway do nadmiarowego kontrolera centrali, można zastosować następującą topologię.

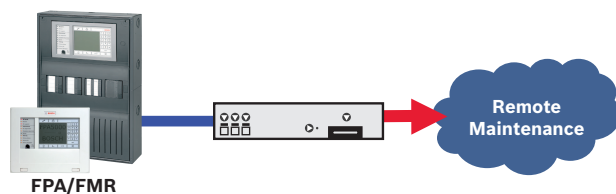


Podstawowe instrukcje konfiguracji Remote Services można znaleźć w rozdziale *Remote Services krok po kroku, Strona 35*

3.7

Remote Maintenance

Remote Maintenance zapewnia możliwość zdalnego monitorowania określonych parametrów różnych elementów zabezpieczeń podłączonych do centrali sygnalizacji pożaru.



Rysunek 3.13: Remote Maintenance

**Uwaga!**

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

**Uwaga!**

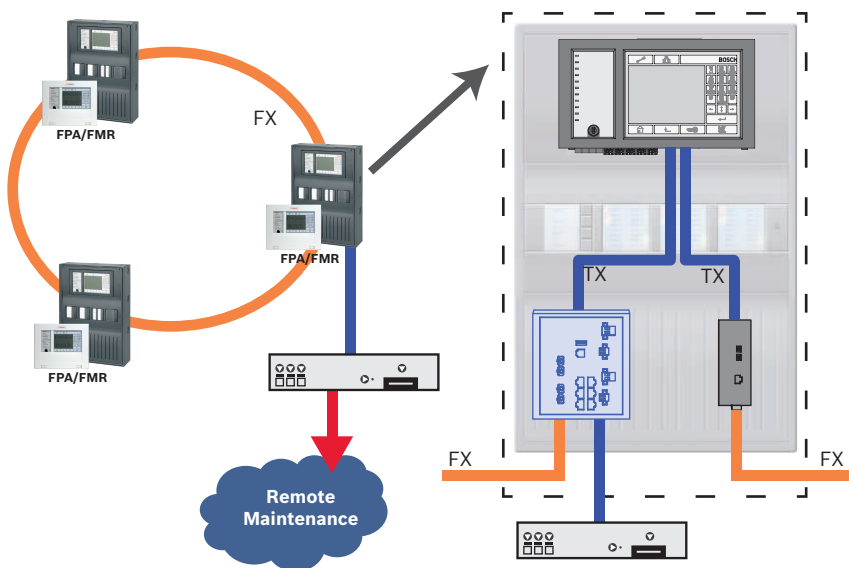
Połączenie używane dla usługi Remote Maintenance nie może być interaktywne.

**Uwaga!**

Należy pamiętać, że dane Remote Maintenance są przesyłane bez szyfrowania.

**Uwaga!**

Do połączenia centrali za pośrednictwem FX można używać tylko konwerterów transmisji.



Rysunek 3.14: Remote Maintenance

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

Usługa Remote Maintenance dla Remote Portal

Remote Maintenance można skonfigurować dla Remote Portal: usługa Remote Maintenance gromadzi dane dotyczące urządzeń LSN oraz modułów funkcyjnych i przesyła je do Remote Portal, gdzie są one analizowane na potrzeby usług Remote Services.

Podstawowe instrukcje konfiguracji Remote Services można znaleźć w rozdziale *Remote Services krok po kroku, Strona 35*

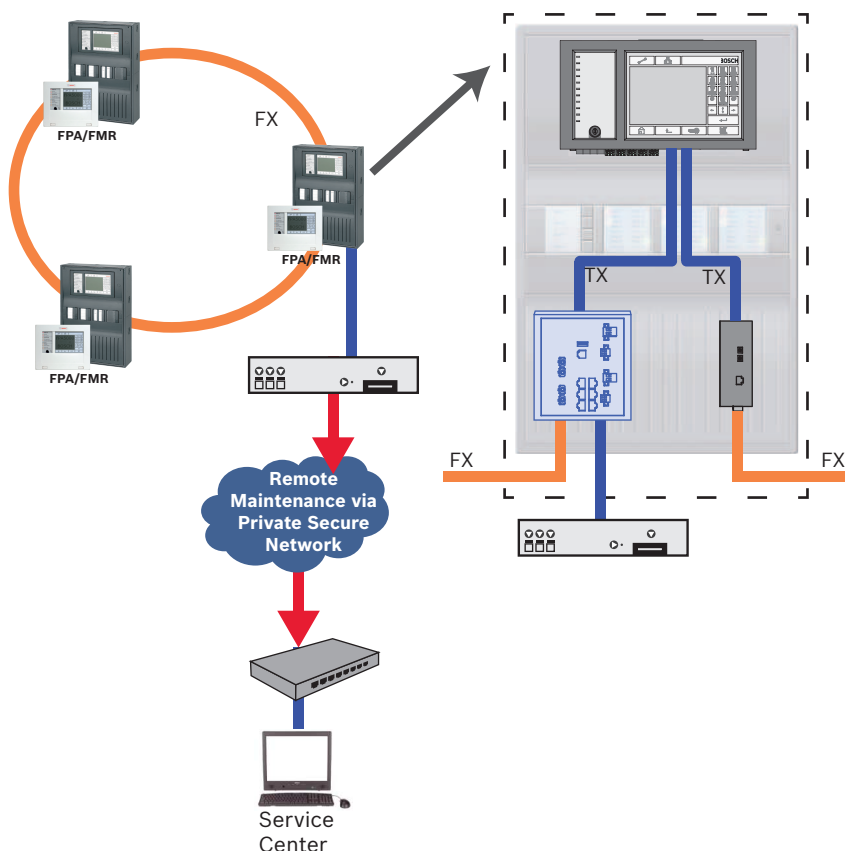
Usługa Remote Maintenance dla sieci Private Secure Network

Przestroga!



Usługa Remote Maintenance for Private Secure Network wymaga bezpiecznego połączenia IP. Z tego powodu w przypadku usługi Remote Maintenance for Private Secure Network dostępna jest sieć IP oparta na DSL z opcjonalnym bezprzewodowym dostępem po stronie centrali. Usługa Remote Maintenance for Private Secure Network jest dostępna tylko w Niemczech wraz z umową o świadczenie usług zawartą z firmą Bosch ST-IE.

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



Rysunek 3.15: 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 centrali do sieci.

Przełącznik do podłączania systemu CMS musi być zaprogramowany oddzielnie.

Aby uzyskać informacje o programowaniu ustawień adresu IP i nadmiarowości przełącznika, patrz *Ustawienia przełącznika, Strona 45*. Ze względu na to, że przełącznik jest instalowany w bezpośrednim sąsiedztwie (bez wolnej przestrzeni), nie jest konieczne projektowanie nadmiarowego zasilania. Dlatego też wyjścia sygnału awarii nie są używane.

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

3.8

Remote Alert

Poprzez Remote Alert centrala przesyła informacje o stanie do Remote Portal. Remote Alert analizuje te dane. W przypadku nieoczekiwanego zdarzenia Remote Portal powiadamia użytkownika za pośrednictwem wiadomości SMS i/lub e-mail o otrzymanych alertach. Podstawowe instrukcje konfiguracji Remote Services można znaleźć w rozdziale *Remote Services krok po kroku*, Strona 35

4 Połączenie z magistralą CAN

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

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

Centrale można połączyć w sieć nadmiarowo jako pętlę za pośrednictwem CAN1 i CAN2.

Połączenie z magistralą FOC

Centrale w pętli mogą być połączone przy użyciu kabli światłowodowych za pośrednictwem adapterów CAN/FOC.

Konwertery CAN/FOC z EKS umożliwiają zwiększenie odległości pomiędzy dwoma węzłami sieci powyżej 15 km (w zależności od użytego typu konwertera i kabla światłowodowego).

Dostępne są następujące konwertery (system PzP CAN FOC/MM):

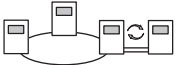
- System DL-CAN/1x13-MM-ST
- System DL-CAN/1x13-MM-SC
- System DL-CAN/1x13-SM-ST
- System DL-CAN/1x13-SM-SC

Topologia pętli

- W topologii pętli kabel CAN zawsze prowadzi od terminalu CAN1 do terminalu CAN2 [CAN1 ⇒ CAN2].
Tak więc segment CAN składa się z dwóch użytkowników magistrali. Długość kabla zależy od przekroju poprzecznego kabla.
- Ze względu na to, że maksymalna liczba węzłów to 32, a maksymalna długość kabla pomiędzy węzłami wynosi 1000 m, system może być zainstalowany przy użyciu kabla o maksymalnej długości 32 km.

Połączenie z siecią central i zdalnych klawiatur

Poniższa tabela przedstawia opcje połączenia z siecią central/zdalnych klawiatur w zależności od topologii sieci.

Topologia		FPA-1200	FPA-5000
	Samodzielna centrala	Możliwe	Możliwe
	Samodzielna centrala, nadmiarowa	Niemożliwe	Możliwe
	Pętla	1 FPA-1200 + maks. 3 FMR-5000	Maks. 32 FPA-5000/FMR-5000
	Pętla z centralą nadmiarową	Niemożliwe	Maks. 32 FPA-5000/FMR-5000 + nadmiarowa FPA-5000
Patrz ograniczenia wynikające z topologii sieci. Centrala FPA-1200 nie pełni roli centrali nadmiarowej, dlatego mikroprzełącznik DIP 6 nie działa w FPA-1200-MPC.			

Ograniczenia w sieci

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

Połączone w sieć centrale i zdalne klawiatury to tzw. węzły.

- Liczba punktów detekcji w sieci jest ograniczona do 32 768.
- Liczba punktów detekcji na centralę działającą w sieci jest ograniczona do 2048.
- Liczba węzłów w systemie zależy od typu topologii.
Węzłem jest albo kontroler centrali MPC, albo zdalna klawiatura FMR-5000.
- Liczba węzłów w topologii pętli jest ograniczona do 32.
- Liczba węzłów na segment CAN jest ograniczona do ośmiu.
Segmentem CAN jest fizyczne połączenie linii CAN.
- Aplikacja do programowania FSP-5000-RPS umożliwia przypisanie do sieci maksymalnie trzech zdalnych klawiatur dla określonej centrali.

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

Typ kabla dla połączenia z siecią

Połączenie CAN to połączenie dwużyłowe (CAN-H i CAN-L). 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. Ekranowany kabel CAN jest podłączony jedynie do metalowej obudowy z jednej strony.

Długość kabla dla połączenia z siecią

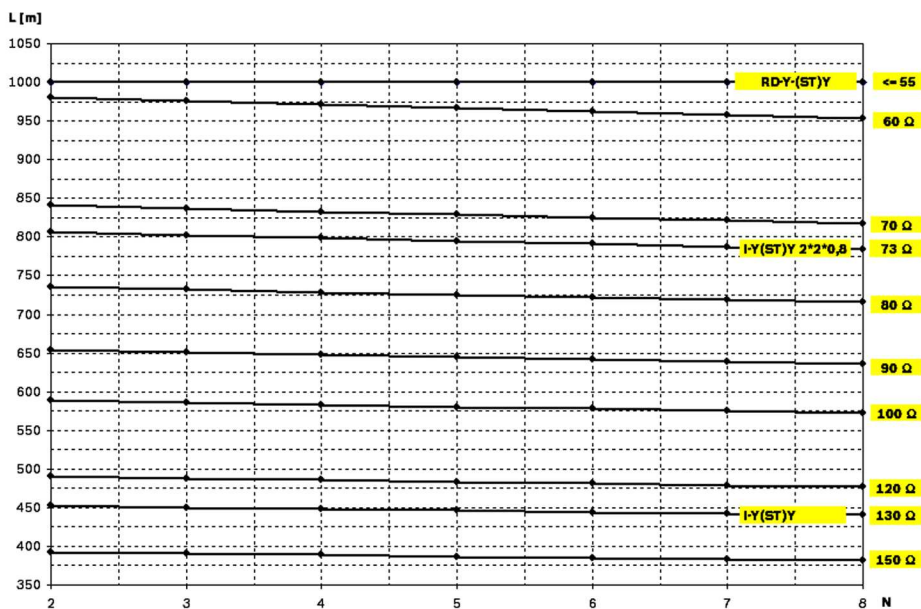
Maksymalna dozwolona długość kabla zależy od rezystancji pętli użytego kabla i liczby komunikujących się węzłów.

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 4.1: Sieć: Długość kabla. Dopuszczalna długość kabla zależna od liczby węzłów i oporności kabla

L = długość kabla w metrach

N = liczba węzłów

4.1

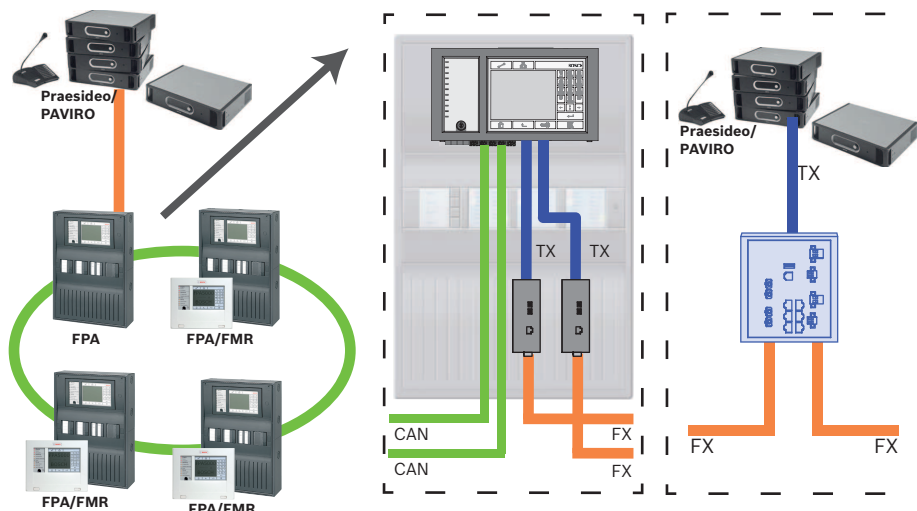
Połączenie z dźwiękowym systemem alarmowym



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).

W każdym kontrolerze centrali sieci CAN można podłączyć jeden system Praesideo/PAVIRO za pomocą interfejsu Ethernet. Poniższa topologia przedstawia połączenie kontrolerów centrali poprzez CAN, gdzie system Praesideo/PAVIRO jest podłączony do jednego kontrolera za pomocą interfejsu sieci Ethernet.



Rysunek 4.2: Połączenie Praesideo/PAVIRO z siecią CAN



Uwaga!

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

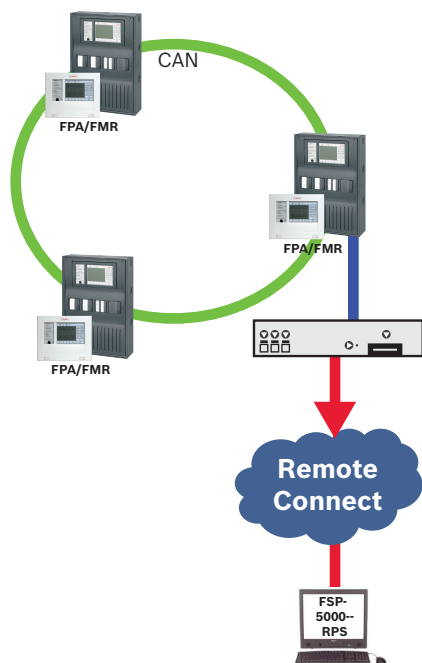
4.2

Remote Connect

Usługa Remote Connect zapewnia bezpieczne połączenie internetowe, które umożliwia zdalny dostęp do centrali. W przypadku usługi Remote Connect należy skorzystać z bezpiecznej bramy sieciowej Secure Network Gateway (CTN: C1500).

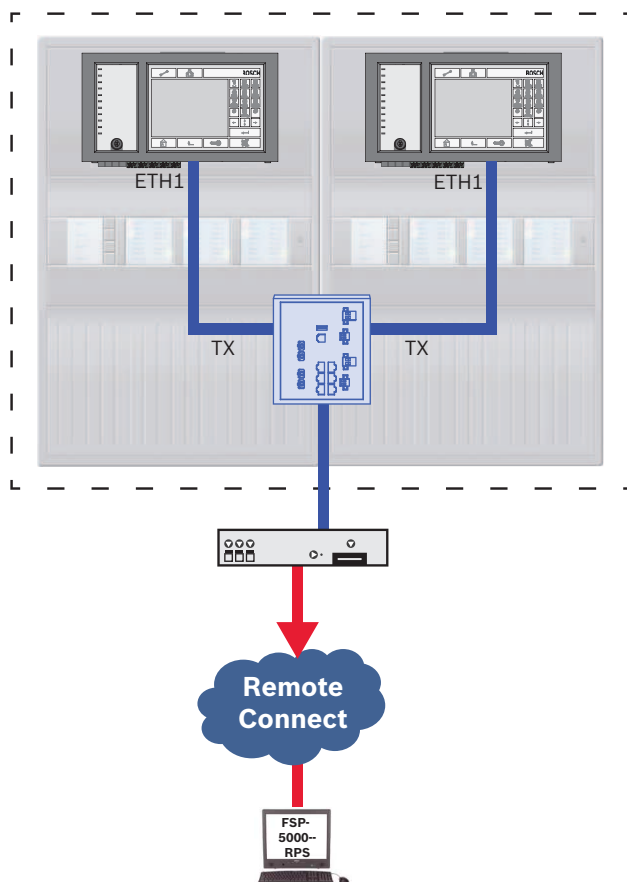
W przypadku sieci central jedna z centrali w sieci musi być podłączona do bezpiecznej bramy sieciowej Secure Network Gateway. To połączenie powinno być dedykowanym połączeniem Ethernet. Usługa Remote Connect musi być włączona w konfiguracji FSP-5000-RPS tej centrali.

Poniższa topologia pokazuje sieć CAN, w której Secure Network Gateway jest podłączona do sieci za pośrednictwem portu Ethernet.



Rysunek 4.3: Remote Connect w pętli CAN

Aby podłączyć Secure Network Gateway do nadmiarowego kontrolera centrali, można zastosować następującą topologię.



Podstawowe instrukcje konfiguracji Remote Services można znaleźć w rozdziale *Remote Services krok po kroku*, Strona 35

5 Remote Services krok po kroku

W tym rozdziale znajdują się podstawowe instrukcje dotyczące konfiguracji usług Remote Services na stronie <https://remote.boschsecurity.com>. Aby używać usług Remote Services, trzeba być użytkownikiem konta Remote Portal. (Do jednego konta Remote Portal może być przypisanych wielu użytkowników). Każde konto Remote Portal ma jeden niepowtarzalny identyfikator Remote ID.



Uwaga!

Usługi Remote Services powinny działać bez ponownej konfiguracji lub regulacji, jeśli są spełnione następujące wymagania:

- centrala z oprogramowaniem sprzętowym w wersji 2.14.7 lub nowszym, interfejsy Ethernet włączone przy standardowych ustawieniach Ethernet
- nieskonfigurowany kontroler centrali lub włączona usługa Remote Connect w konfiguracji centrali FSP-5000-RPS
- dostępna bezpieczna brama sieciowa Secure Network Gateway dla usług Remote Services
- komputer z aplikacją do programowania FSP-5000-RPS w wersji 4.8 lub wyższej i dostępem do Internetu



Uwaga!

Zaleca się określenie strefy czasowej w bezpiecznej bramie sieciowej Secure Network Gateway.

Mechanizm aktualizacji bezpiecznej bramy sieciowej Secure Network Gateway zapewnia regularne aktualizacje. Aby uniknąć aktywności związanej z aktualizacją podczas połączenia, należy określić strefę czasową w obszarze **System -> General Settings -> Timezone** (System -> Ustawienia ogólne -> Strefa czasowa).

Krok 1: Utwórz konto Remote Portal

Aby korzystać z usług Remote Services, należy być użytkownikiem konta Remote Portal. Każde konto Remote Portal ma jeden niepowtarzalny identyfikator Remote ID. Każdy identyfikator Remote ID jest przeznaczony dla jednej firmy. Jeśli nie masz identyfikatora Remote ID, wykonaj następujące czynności:

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

Aby zapewnić oddzielne konta dla techników, można utworzyć kilku użytkowników dla tego samego identyfikatora Remote ID:

Zaloguj się do Remote Portal.

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

Krok 2: Podłącz bezpieczną bramę sieciową Secure Network Gateway

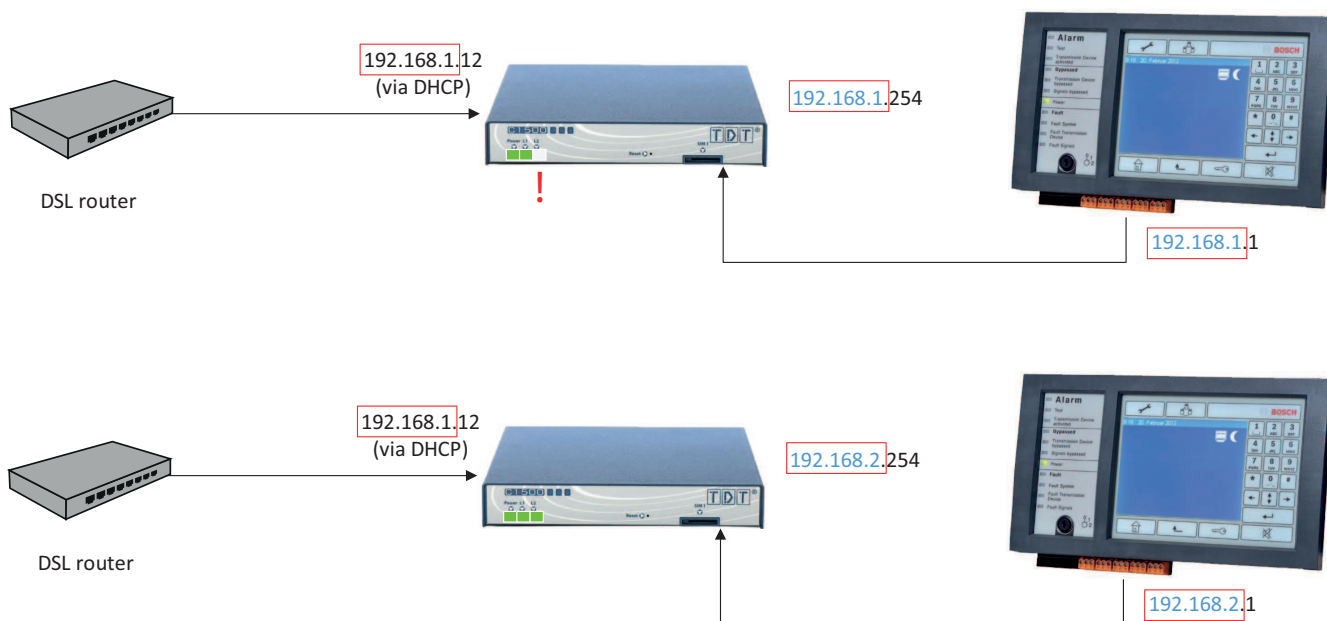
Aby używać usług Remote Services, należy skorzystać z bezpiecznej bramy sieciowej Secure Network Gateway (C1500).

1. Podłącz port bezpiecznej bramy sieciowej eth0 Secure Network Gateway do routera internetowego lub sieci firmowej z dostępem do Internetu.
2. Podłącz port bezpiecznej bramy sieciowej eth1 Secure Network Gateway do jednego z portów Ethernet kontrolera centrali za pomocą dołączonego kabla sieciowego CAT5 RJ45. Dostępne topologie można sprawdzić w rozdziałach *Połączenie z siecią Ethernet, Strona 7* i *Połączenie z magistralą CAN, Strona 31*.
3. Podłącz bezpieczną bramę sieciową Secure Network Gateway do zasilania sieciowego 100 V - 230 V za pomocą zasilacza.

Po nawiązaniu połączenia z Internetem dioda LED L1 zapala się na zielono. Wkrótce potem na zielono zaczyna świecić dioda LED L2, co oznacza, że zostało nawiązane połączenie VPN z Remote Portal.

Rozdzielanie podsieci (dioda LED L2 wył.)

Podłączenie bezpiecznej bramy sieciowej Secure Network Gateway dla usług Remote Services nie powiedzie się w przypadku nakładających się podsieci (dioda LED L2 wył.). Poniższy przykład przedstawia bezpieczną bramę sieciową Secure Network Gateway i kontroler centrali znajdujące się w tym samym zakresie adresów co router DSL.



Bezpieczna brama sieciowa Secure Network Gateway z najnowszym oprogramowaniem sprzętowym wykrywa jednoznacznie nakładające się podsieci: dioda LED Power 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 Secure Network Gateway. 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 domyślnej bramy **Brama domyślna**: w konfiguracji kontrolera centrali musi być zgodny z adresem IP bezpiecznej bramy sieciowej Secure Network Gateway.

Krok 3: Nawiąż połączenie zdalne

1. W centrali użyj standardowych ustawień sieci Ethernet, patrz *Standardowe ustawienia Ethernet dotyczące FPA, Strona 13*.
2. Zrestartuj centralę.
3. Do uwierzytelnienia wybierz **Configuration** -> **Network Services** -> **Change date / time** (Konfiguracja -> Usługi sieciowe -> Zmień datę/godzinę), wpisz bieżącą datę i potwierdź ustawienia.
4. Wybierz **Configuration** -> **Network Services** -> **Remote Services** (Konfiguracja -> Usługi sieciowe -> Remote Services), a następnie wpisz identyfikator Remote ID.

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

Krok 4: Przypisz licencję w Remote Portal

Aby korzystać z usług Remote Services, należy przypisać licencję dołączoną do bezpiecznej bramy sieciowej Secure Network Gateway.

**Uwaga!**

Raz przypisaną licencję nie da się przypisać ponownie ani zawiesić.

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

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

Krok 5: Zamów ponownie licencję

- ▶ Zamów jednoroczne licencje w BOSCH Fire Alarm Systems. Każda sieć wymaga własnych licencji.

BOSCH wyśle wiadomość e-mail na podany adres. W wiadomości znajdują się niepowtarzalne numery do zarejestrowania zamówionych licencji, a także instrukcje i łącze do Remote Portal.

1. Na stronie <https://remote.boschsecurity.com> -> **Login** (Zaloguj się), wpisz swój adres e-mail i hasło.
 2. Wybierz **Licenses** (Licencje).
 3. Kliknij przycisk **+**.
 4. Postępuj zgodnie z instrukcjami wyświetlonymi w oknie **Add Licenses** (Dodaj licencje) i potwierdź, klikając przycisk **Save** (Zapisz).
- Lista licencji zostanie zaktualizowana.

6 Ustawienia protokołu RPS

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

Innym możliwym rozwiązaniem jest wykorzystanie interfejsu sieciowego przełącznika podłączonego do sieci.

6.1 Węzły sieci

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

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

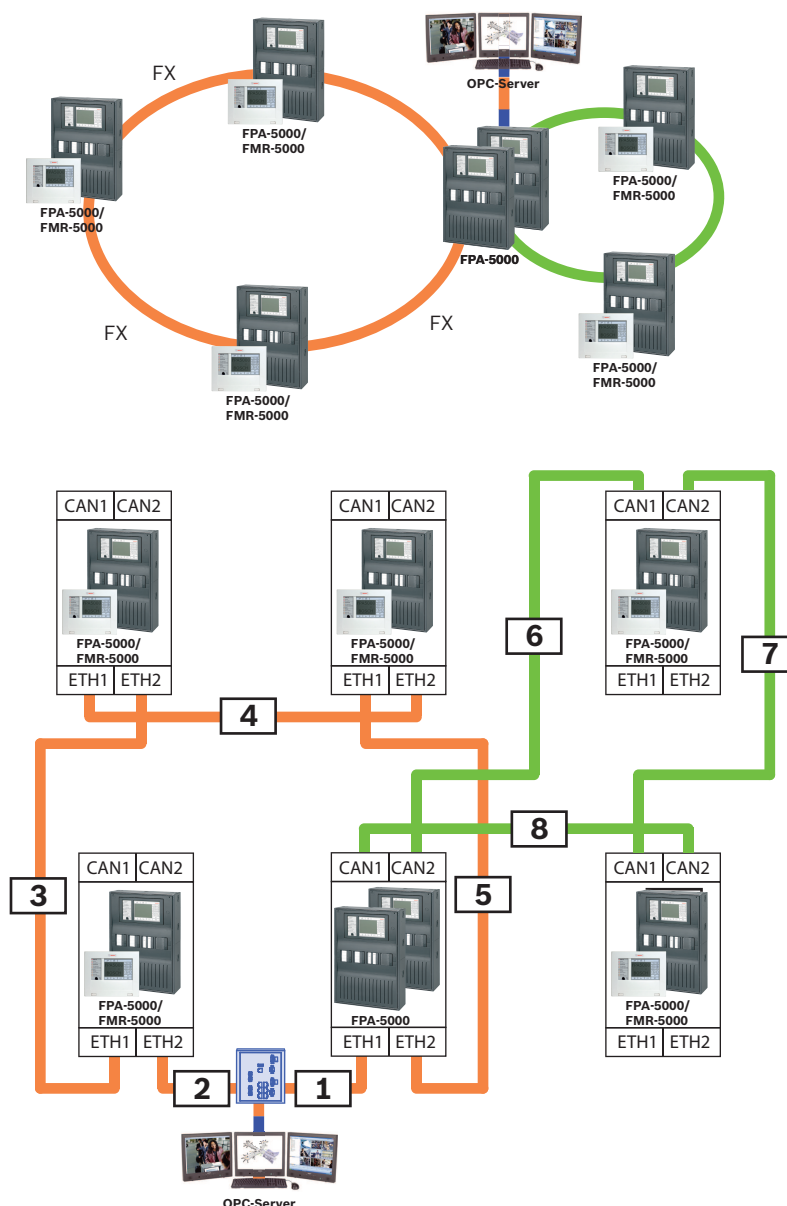
Po ponownym uruchomieniu sieci należy sprawdzić komunikaty o błędach i w razie potrzeby naprawić ewentualne błędy.

6.2 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 6.1: Przykład sieci i możliwe numerowanie linii

6.3

Przełączniki

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

6.4

Serwery OPC

Jeśli w sieci używane są serwery OPC, należy je dodać do aplikacji do programowania RPS. W oprogramowaniu RPS i na serwerze OPC muszą być skonfigurowane następujące ustawienia:

- Węzły sieci
- Grupa sieciowa
- RSN
- Adres IP

- Port
- Standardowo serwer OPC używa portu 25000.

**Uwaga!**

Aplikacja do programowania FSP-5000-RPS:

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

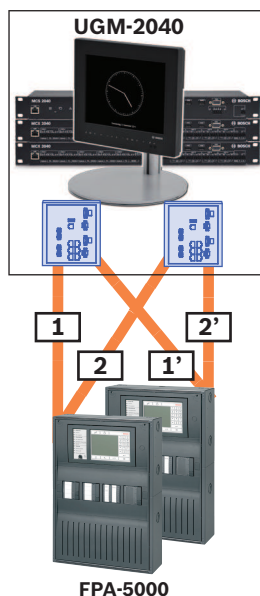
6.5 Serwery UGM-2040

**Uwaga!**

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

W przypadku wielu konfiguracji FPA lub sieci muszą one znajdować się w tej samej podsieci. Adresy multimedii powinny się różnić.

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



Rysunek 6.2: Przykład numerowania linii dla UGM-2040

**Uwaga!**

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

7 Instalacja

Lista kontrolna

Przed rozpoczęciem instalacji sieci należy sprawdzić wszystkie poniższe punkty.

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

Niebezpieczeństwo!

Światło lasera.

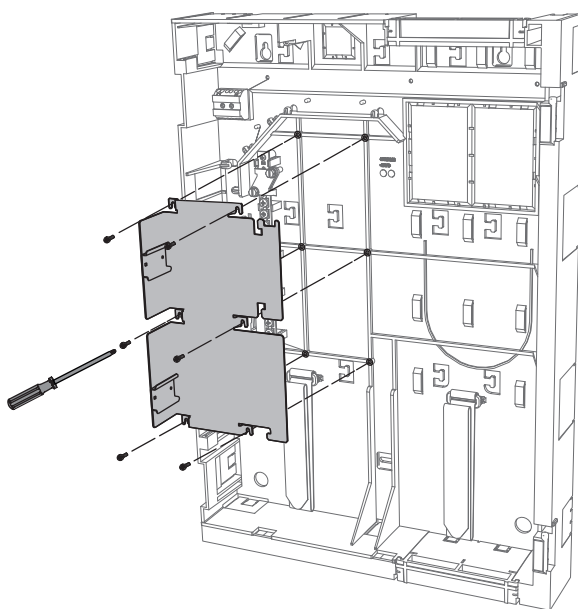


Nie należy patrzeć wprost na wiązkę nieuzbrojonym okiem ani przez przyrządy optyczne dowolnego rodzaju (np. przez szkło powiększające lub mikroskop). Zlekceważenie tego zalecenia jest niebezpieczne dla oczu, zwłaszcza przy odległościach mniejszych niż 100 mm. Wiązka świetlna jest obecna w terminalach optycznych i na końcach podłączonych do nich kabli światłowodowych. Fotodioda CLASS 2M, długość fali 650 nm, wyjście < 2 mW (zgodnie z normą DIN EN 60825-1:2003-10).

7.1 Instalacja konwerterów transmisji w ramie montażowej

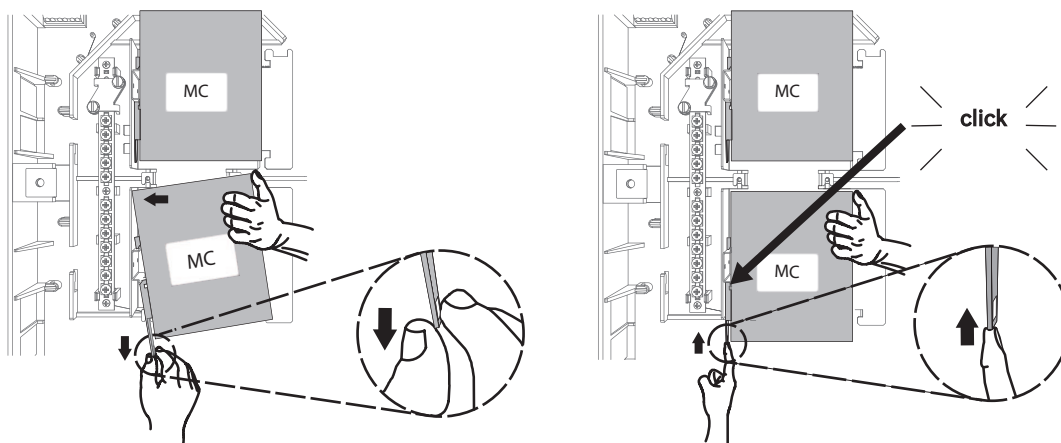
Należy zainstalować konwertery transmisji w odpowiednim uchwycie FPM-5000-KMC.

 6x KB40 x 12 mm



FBH 0000 A
(FHS 0000 A)

Rysunek 7.1: Instalacja uchwytu FPM-5000-KMC w ramie montażowej



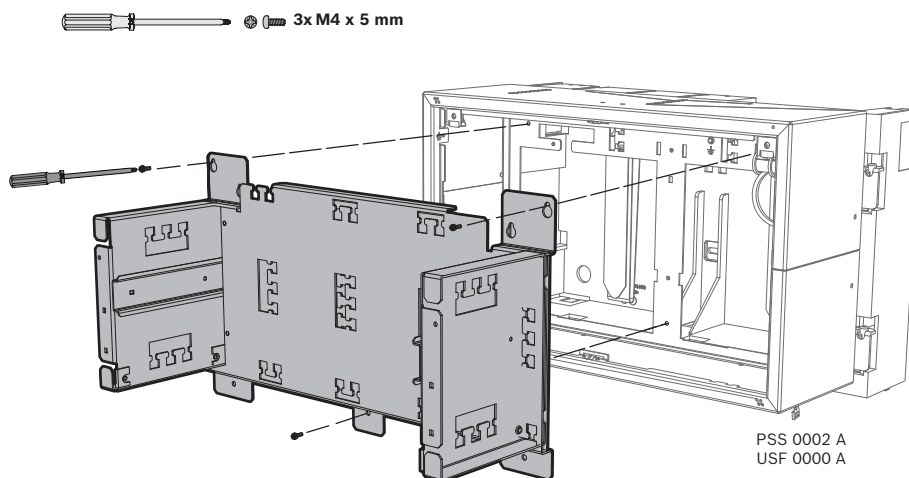
Rysunek 7.2: Instalacja konwerterów transmisji w uchwycie FPM-5000-KMC

7.2

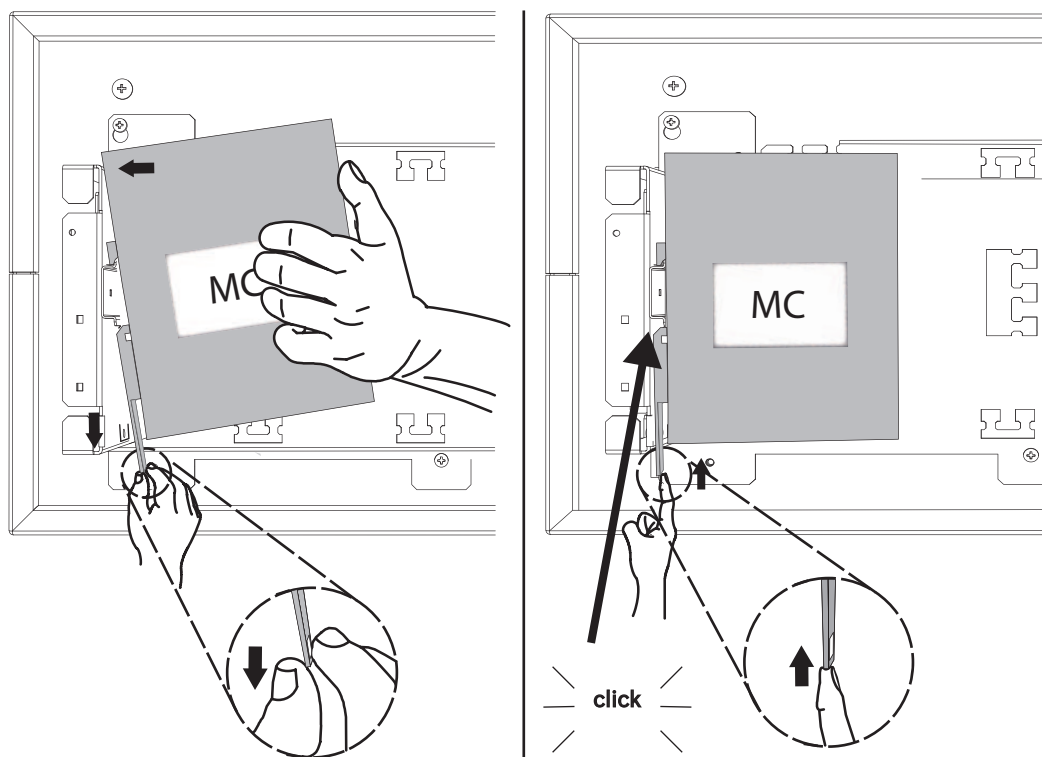
Instalacja konwerterów transmisji w PSS 0002 A/USF 0000 A

Należy zainstalować konwertery transmisji w uchwycie FPM-5000-KES.

W przypadku USF 0000 A trzeba usunąć zainstalowaną płytę montażową.



Rysunek 7.3: Instalacja uchwytu FPM-5000-KES w obudowach



Rysunek 7.4: Instalacja konwerterów transmisji w uchwycie FPM-5000-KES

7.3

Ustawienia konwertera transmisji

Użycie konwertera transmisji wymaga wykonania tylko kilku czynności:

- Ustaw przełączniki DIP.
- Podłącz konwerter transmisji do kabli sieciowych FX i CAT5e.
- Podłącz konwerter transmisji do zasilania za pośrednictwem wewnętrznego modułu kontrolera akumulatorów BCM.



Uwaga!

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



Uwaga!

Instalacje sieciowe wymagają korzystania wyłącznie z następujących kabli:

Kabel Ethernet

Kabel sieciowy Ethernet, ekranowany, CAT5e lub lepszy.

Należy pamiętać o minimalnym promieniu zgięcia określonym w specyfikacji kabla.

Kabel światłowodowy

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

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

Należy pamiętać o minimalnym promieniu zgięcia określonym w specyfikacji kabla.



Uwaga!

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

**Uwaga!**

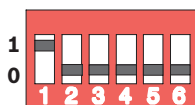
W przypadku wielomodowych konwerterów transmisji maksymalna długość odcinka transmisji za pośrednictwem FX wynosi 2000 m.

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

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

**Uwaga!**

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



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

7.4

Instalowanie przełączników w PSS 0002 A/USF 0000 A

**Uwaga!**

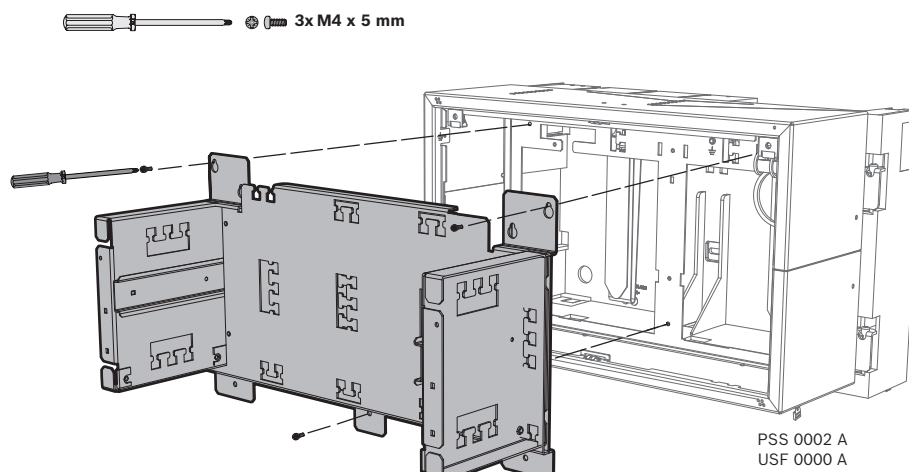
W przypadku używania przełączników w sieci central FPA-5000 należy to uwzględnić w konfiguracji w aplikacji do programowania FSP-5000-RPS.

**Uwaga!**

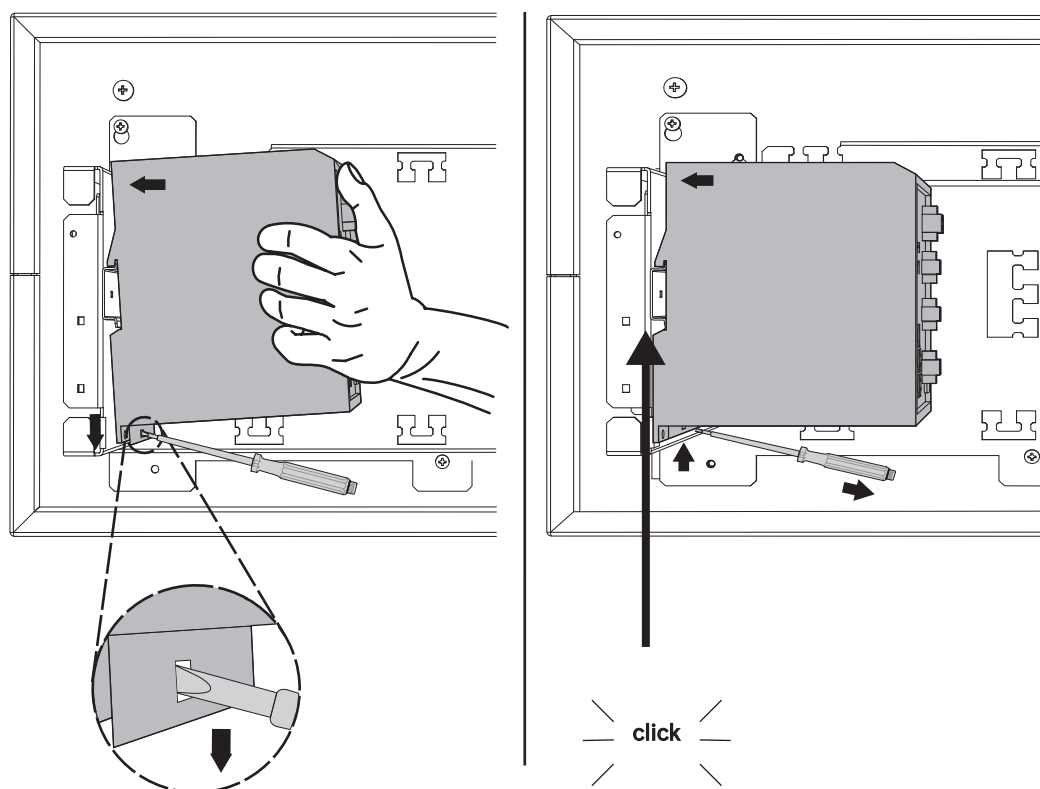
Przełączników nie należy podłączać za pomocą dostarczonego kabla sieciowego, ponieważ jest on nieekranowany.

Należy użyć kabla sieciowego Ethernet, ekranowanego, CAT5e lub lepszego.

Należy zainstalować przełączniki w odpowiednim uchwycie FPM-5000-KES.



Rysunek 7.5: Instalacja uchwytu FPM-5000-KES w obudowach



Rysunek 7.6: Instalacja przełączników w uchwycie FPM-5000-KES

7.5

Ustawienia przełącznika

Aby umożliwić użycie przełączników w sieci, trzeba je zaprogramować.

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

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

**Uwaga!**

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

Dane dostępowe:

Użytkownik: admin

Hasło: private

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

Skonfiguruj następujące ustawienia:

- Przypisanie adresu IP, Strona 46,
- Programowanie ustawień nadmiarowości, Strona 47.

Ponadto dostępne są ustawienia opcjonalne, np.:

- Programowanie przekaźnika usterki, Strona 47,
- Programowanie monitoringu połączeń, Strona 48,
- Jak włączyć śledzenie IGMP, Strona 48.

7.5.1**Przypisanie adresu IP****Uwaga!**

Praktyczna wskazówka:

Jeśli konfiguracja sieciowa to umożliwia, w części adresów IP dotyczących urządzenia dla przełączników należy używać liczb większych niż 200 (xxx.xxx.xxx.200). Zapewni to lepsze odróżnianie adresów IP centrali od adresów IP przełączników.

Przykład:

Przełącznik 192.168.1.201 jest przypisany do centrali o adresie IP 192.168.1.1.

**Uwaga!**

Dokładny opis instalacji i konfiguracji przełączników można znaleźć w następujących dokumentach producenta:

Instrukcja instalacji

Skrócony przewodnik interfejsu internetowego

Za pomocą przeglądarki należy wywołać interfejs użytkownika, aby skonfigurować przełącznik. W menu **Basic Settings -> Network** (Ustawienia podstawowe -> Sieć) ustaw następujące wartości w zależności od wybranej topologii:

- Mode (Tryb): local (lokalny)
- Adres IP: wymagany adres IP, np. 192.168.1.201
- Ekran sieciowy: wymagany ekran sieciowy, np. 255.255.255.0
- Gateway: wymagana brama, np. 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).

7.5.2

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).

7.5.3

Programowanie przełącznika usterki



Uwaga!

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

Istnieje połączenie pomiędzy dwoma przełącznikami. Jest to możliwe, np. w przypadku sieci szkieletowej z podpętlami.

Zasilanie przełącznika jest zaprojektowane nadmiarowo.



Uwaga!

Dokładny opis instalacji i konfiguracji przełączników można znaleźć w następujących dokumentach producenta:

Instrukcja instalacji

Skrócony przewodnik interfejsu internetowego

Za pomocą przeglądarki należy wywołać interfejs użytkownika, aby skonfigurować przełącznik. W obszarze **Diagnosis -> Signal Contact** (Diagnostyka -> Styk sygnału) na karcie **Signal Contact 1** (Styk sygnału 1) ustaw w polu **Signal Contact Mode** (Tryb styku kontaktu) wartość **Device Status** (Stan urządzenia).

W obszarze **Diagnosis -> Device Status** (Diagnostyka -> Stan urządzenia) w polu **Monitoring** ustaw następujące wartości:

- **Power Supply 1** (Zasilacz 1): **Monitor** (Monitoruj)
- **Connection Error** (Błąd połączenia): **Monitor** (Monitoruj)

Dla wszystkich innych ustawień należy wybrać wartość **Ignore** (Ignoruj).



Uwaga!

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

Kliknij przycisk **Write** (Zapisz).

**Uwaga!**

Ustawienia poszczególnych pozycji menu w konfiguracji przełącznika zostaną wprowadzone po kliknięciu przycisku **Write** (Zapisz).

Aby ustawienia zostały zapisane trwale, tzn. były przechowywane nawet po ponownym uruchomieniu urządzenia, należy w obszarze **Basic Settings -> Load/Save** (Ustawienia podstawowe -> Załaduj/Zapisz) w polu **Save** (Zapisz) zaznaczyć pole **On the device** (Na urządzeniu) i kliknąć przycisk **Save** (Zapisz).

7.5.4**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** (Przełącznik 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** (Przełącznik 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).

7.5.5**Priorytet QoS, dotyczy tylko UGM-2040**

W przypadku używania przełączników do wymiany danych pomiędzy sieciami FPA i UGM-2040 konieczne jest ustawienie priorytetu QoS w przełącznikach UGM.

W menu QoS/Priorität -> Global zmień ustawienia pola listy rozwijanej w obszarze Trusted Mode na wartość trustIpdscp.

Kliknij przycisk **Write** (Zapisz).

**Uwaga!**

Ustawienia poszczególnych pozycji menu w konfiguracji przełącznika zostaną wprowadzone po kliknięciu przycisku **Write** (Zapisz).

Aby ustawienia zostały zapisane trwale, tzn. były przechowywane nawet po ponownym uruchomieniu urządzenia, należy w obszarze **Basic Settings -> Load/Save** (Ustawienia podstawowe -> Załaduj/Zapisz) w polu **Save** (Zapisz) zaznaczyć pole **On the device** (Na urządzeniu) i kliknąć przycisk **Save** (Zapisz).

7.5.6**Jak włączyć śledzenie IGMP**

Aby uniemożliwić przesyłanie ruchu multimedialnego zgodnego z normą EN 54-2 do innych systemów połączonych z Hirschmann Ethernet Switch (Praesideo/PAVIRO, Remote Connect), należy aktywować śledzenie IGMP.

Na stronie konfiguracji IGMP dotyczącej Hirschmann 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 multimisji na zapytania IGMP queries (np. 3 sekundy).
5. Wybierz opcję **Discard** (Odrzuć) dla pakietów z nieznanymi adresami multimisji.
6. Wybierz opcję **Send to Query and registered Ports** (Wysyłaj do portów zapytania i zarejestrowanych) dla pakietów o znanych adresach multimisji.
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.

7.6

Sieć CAN

Połączenie z siecią i interfejsy

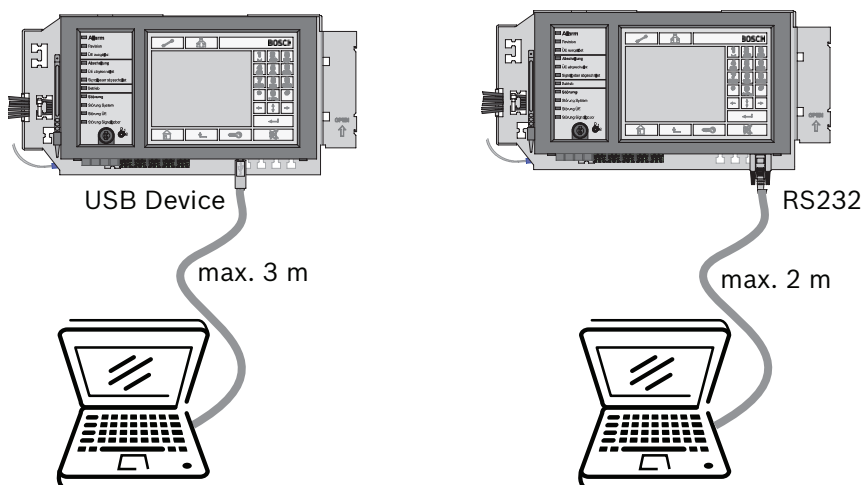
Kontroler centrali ma

- dwa interfejsy CAN (CAN1/CAN2) do połączeń sieciowych (topologia magistrali lub pętli)
- dwa wejścia sygnałowe (IN1/IN2)
- dwa interfejsy Ethernet
- Interfejsy USB i RS232

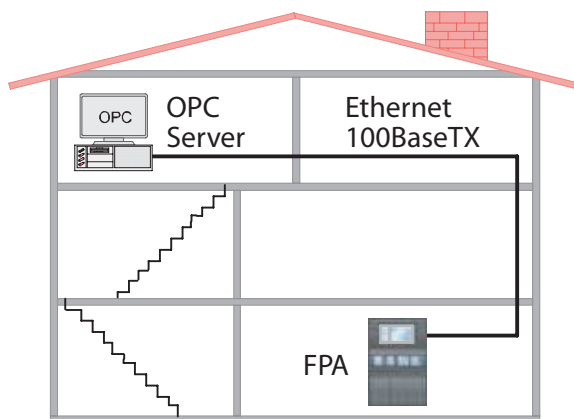
Należy pamiętać, że długość kabla nie może przekraczać 3 m w przypadku podłączenia do interfejsu USB lub 2 m w przypadku podłączenia do interfejsu RS232.

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

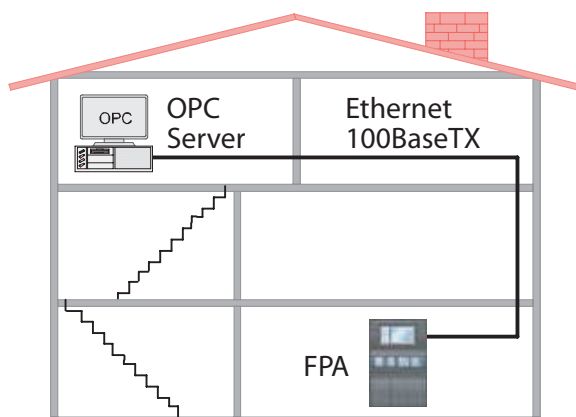
1. sieć taka pozwala na podłączenie do systemu wielu budynków (np. zmiana potencjału masy nie może powodować zakłóceń technicznych);
2. przepustowość użytkowników magistrali jest wystarczająca dla sieci.



Rysunek 7.7: Interfejsy MPC, USB i RS232



Rysunek 7.8: Połączenie MPC z BIS za pośrednictwem serwera OPC



Rysunek 7.9: Połączenie MPC z BIS za pośrednictwem serwera OPC

Adresowanie i ustawienia w sieci

Na kolejnych stronach przedstawiono połączenia, adresowanie i powiązaną konfigurację przy użyciu przełączników DIP w przypadku różnych topologii pętli i magistrali:

- Samodzielna centrala
- Samodzielna centrala, nadmiarowa
- Topologia pętli
- Topologia pętli z centralą nadmiarową
- Topologia magistrali
- Topologia magistrali z centralą nadmiarową
- Topologia magistrali z siecią nadmiarową
- Topologia magistrali z siecią nadmiarową i centralą nadmiarową

Centrale i klawiatury zdalne są identyfikowane w sieci według unikatowego adresu. Adres ten jest ustawiony na przełącznikach obrotowych jako tzw. numer przełącznika obrotowego (RSN) (patrz cyfry w okręgu na schematach obwodu). Przełączniki obrotowe są umieszczone z tyłu kontrolera centrali (patrz *Adresowanie i konfiguracja kontrolera centrali MPC*, Strona 52).

Należy zwrócić uwagę na adres na znaku poniżej przełączników obrotowych (patrz *Adresowanie i konfiguracja kontrolera centrali MPC*, Strona 52, krok 2).

Przełączniki DIP są umieszczone z tyłu kontrolera centrali (patrz *Adresowanie i konfiguracja kontrolera centrali MPC*, Strona 52).

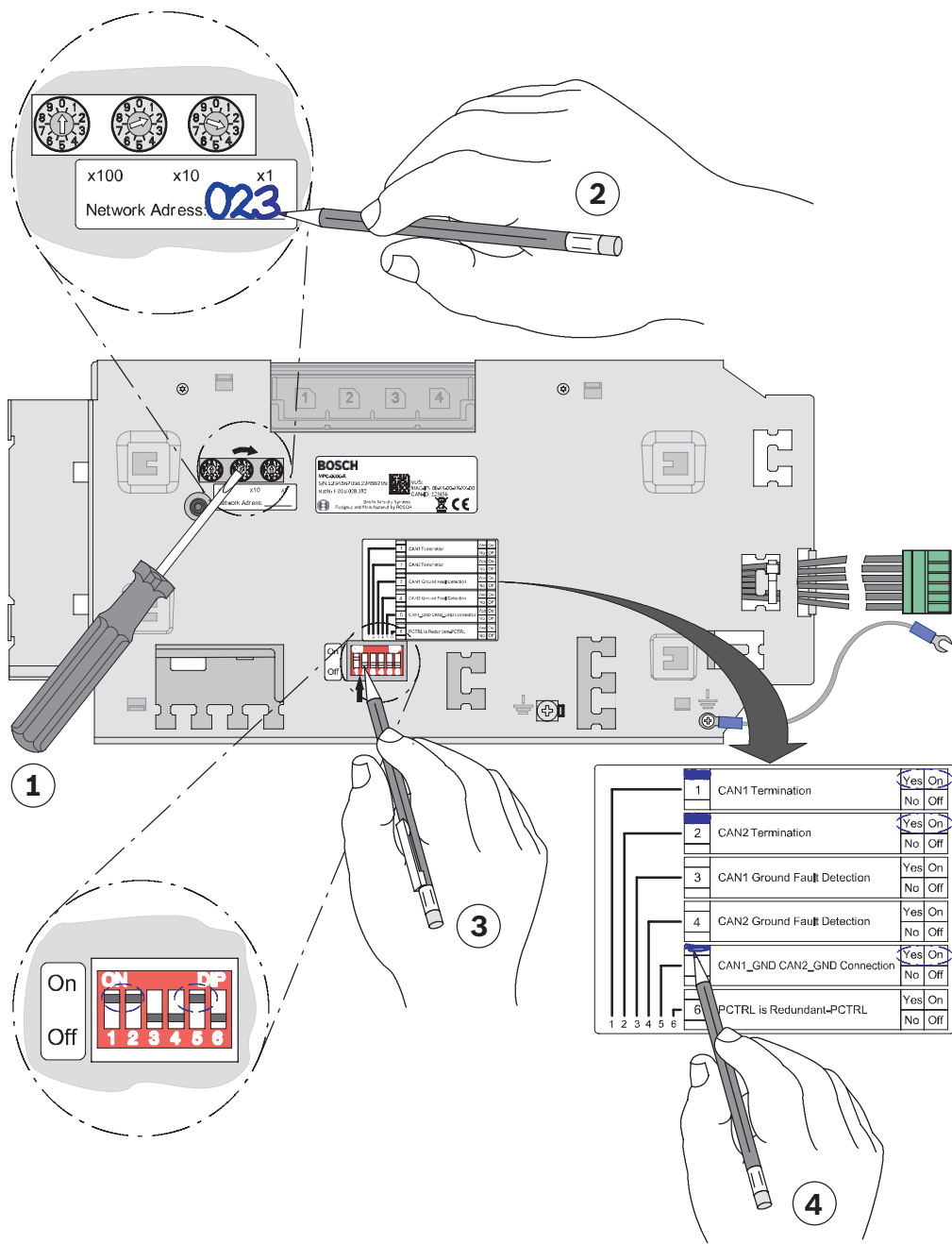
Należy oznaczyć wybrane ustawienie na znaku powyżej przełączników DIP (patrz *Adresowanie i konfiguracja kontrolera centrali MPC*, Strona 52, krok 4).



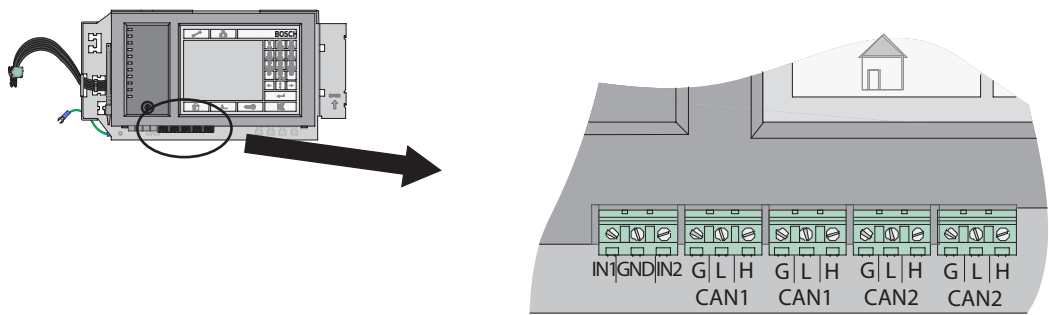
Uwaga!

Centrale nadmiarowe muszą mieć ten sam numer RSN, jak przypisane centrale główne.

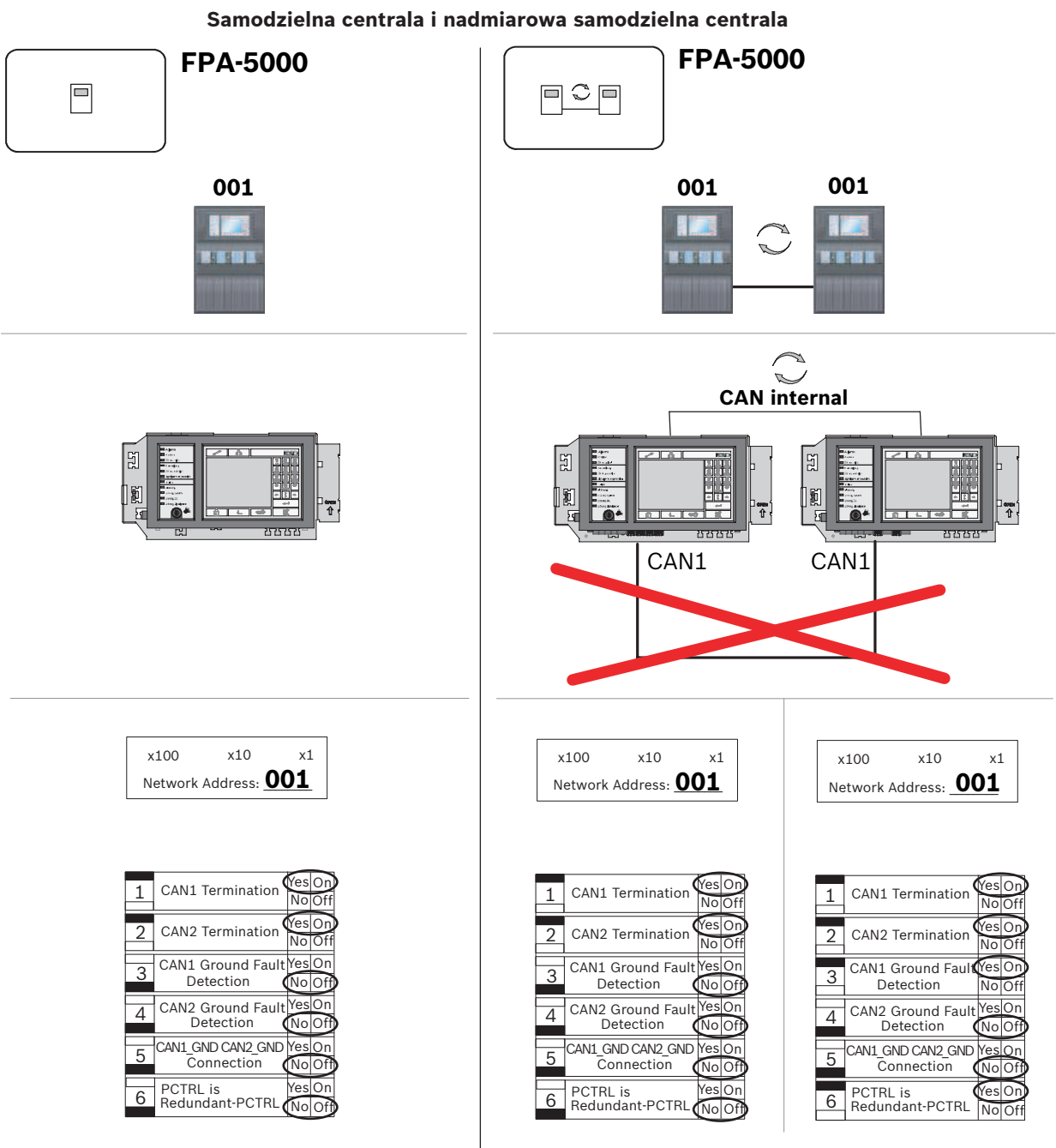
Adresowanie i konfiguracja kontrolera centrali MPC



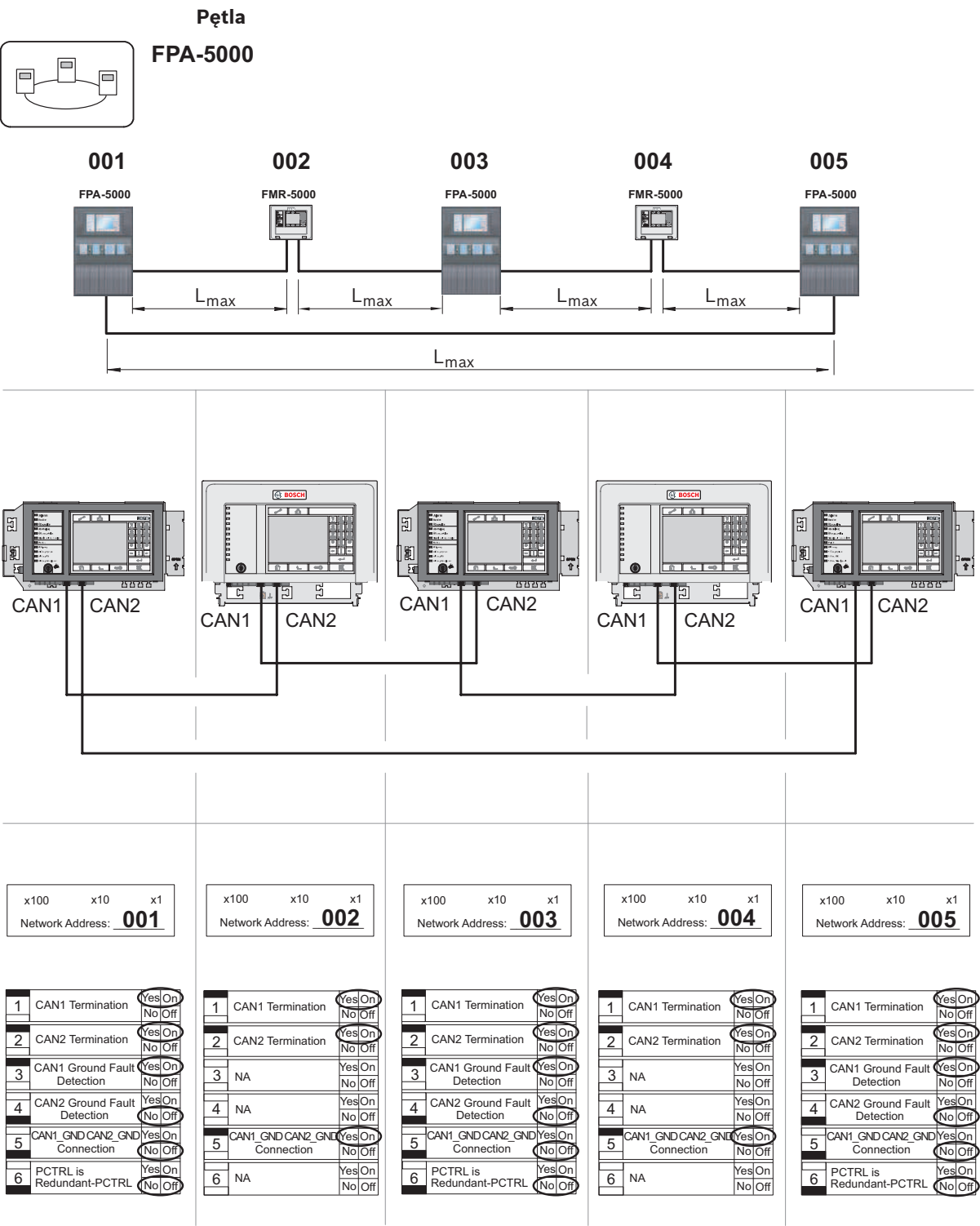
Rysunek 7.10: Kontroler centrali MPC, adresowanie



Rysunek 7.11: Kontroler centrali MPC, połączenia sieciowe

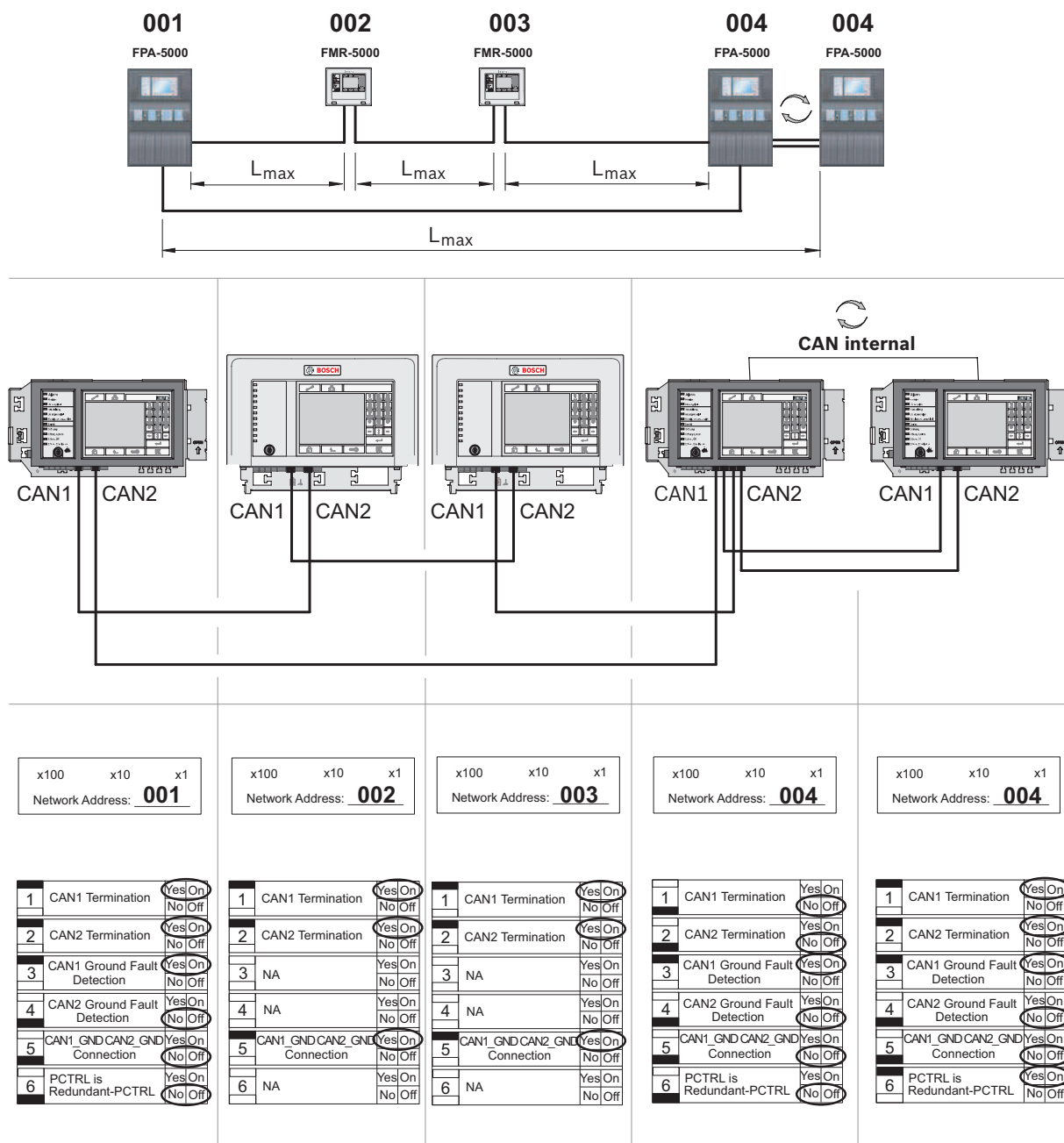
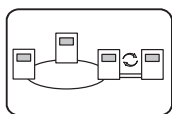


Rysunek 7.12: Samodzielna centrala (zwykła i nadmiarowa): konfiguracja w sieci

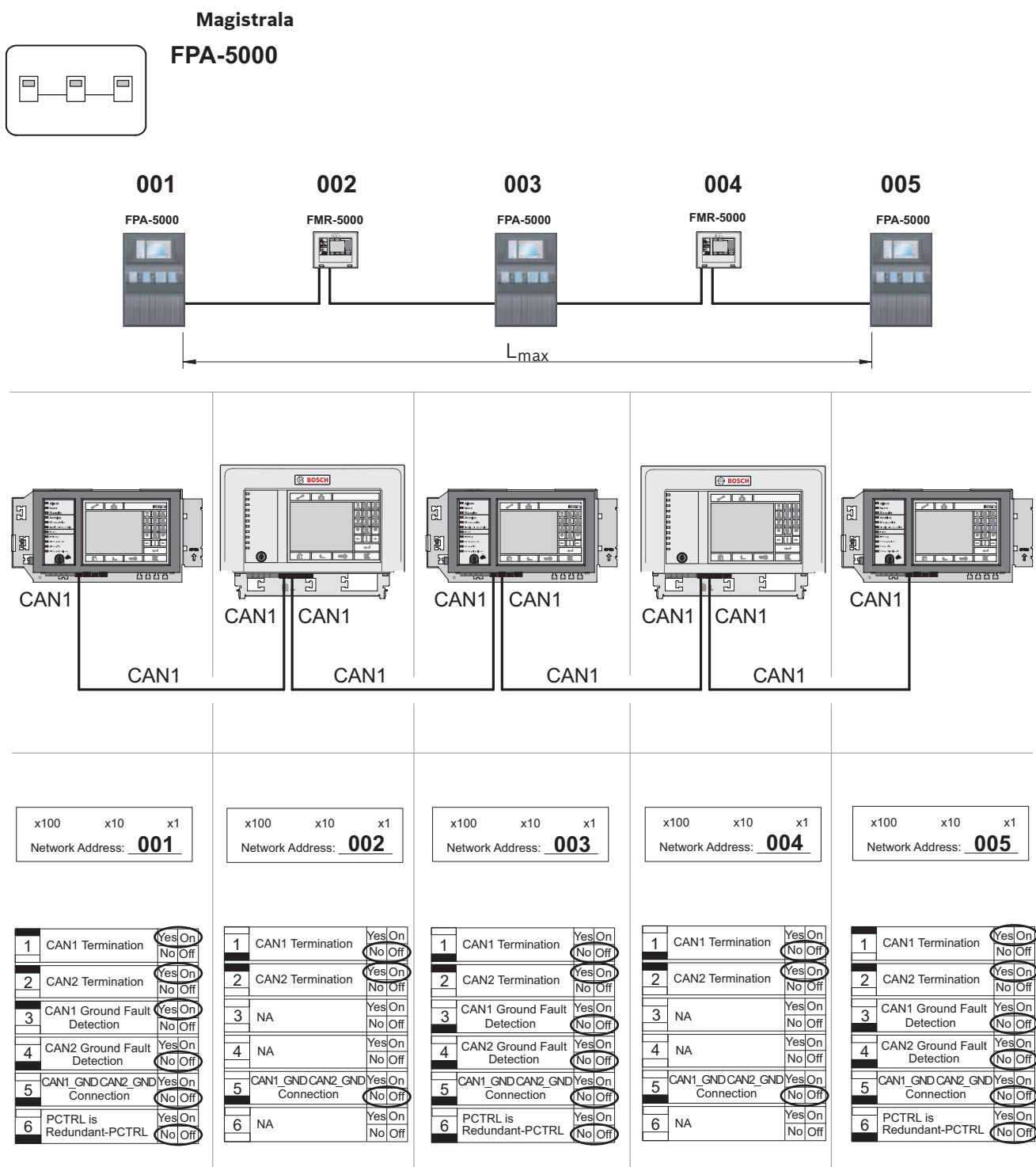


Rysunek 7.13: Topologia pętli

Pętla z centralą nadmiarową FPA-5000

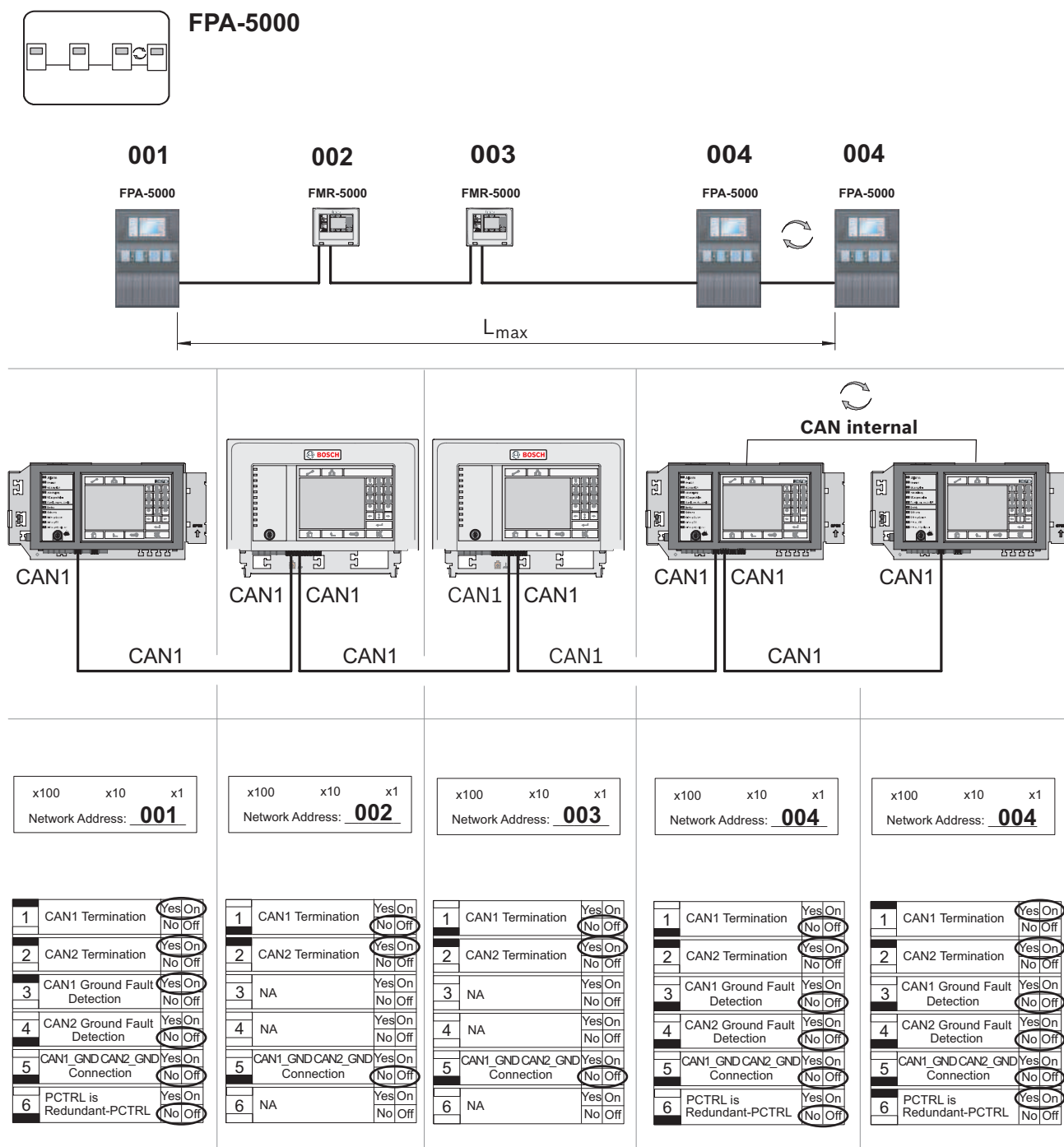


Rysunek 7.14: Topologia pętli z centralą nadmiarową

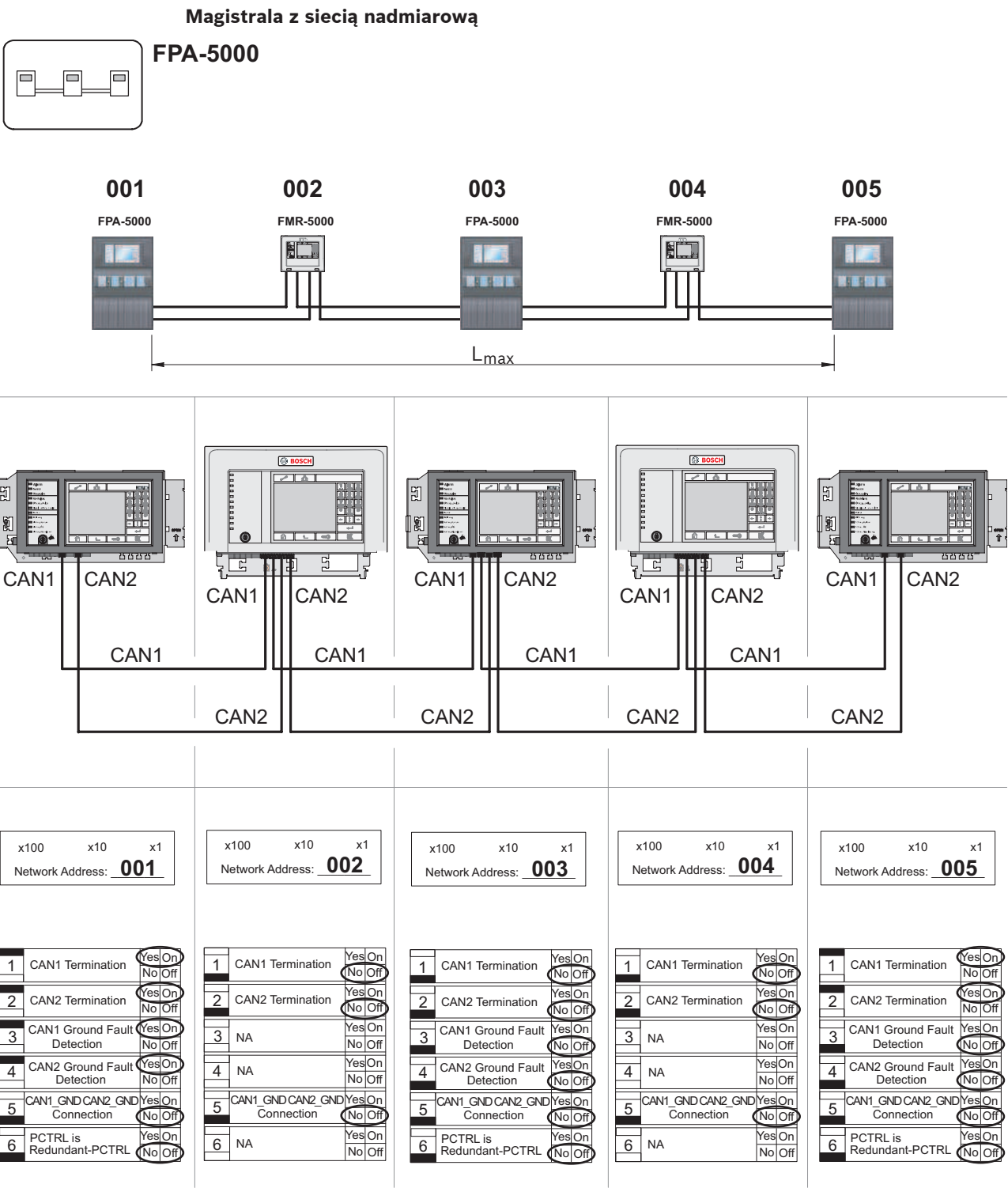


Rysunek 7.15: Topologia magistrali

Magistrala z centralą nadmiarową FPA-5000

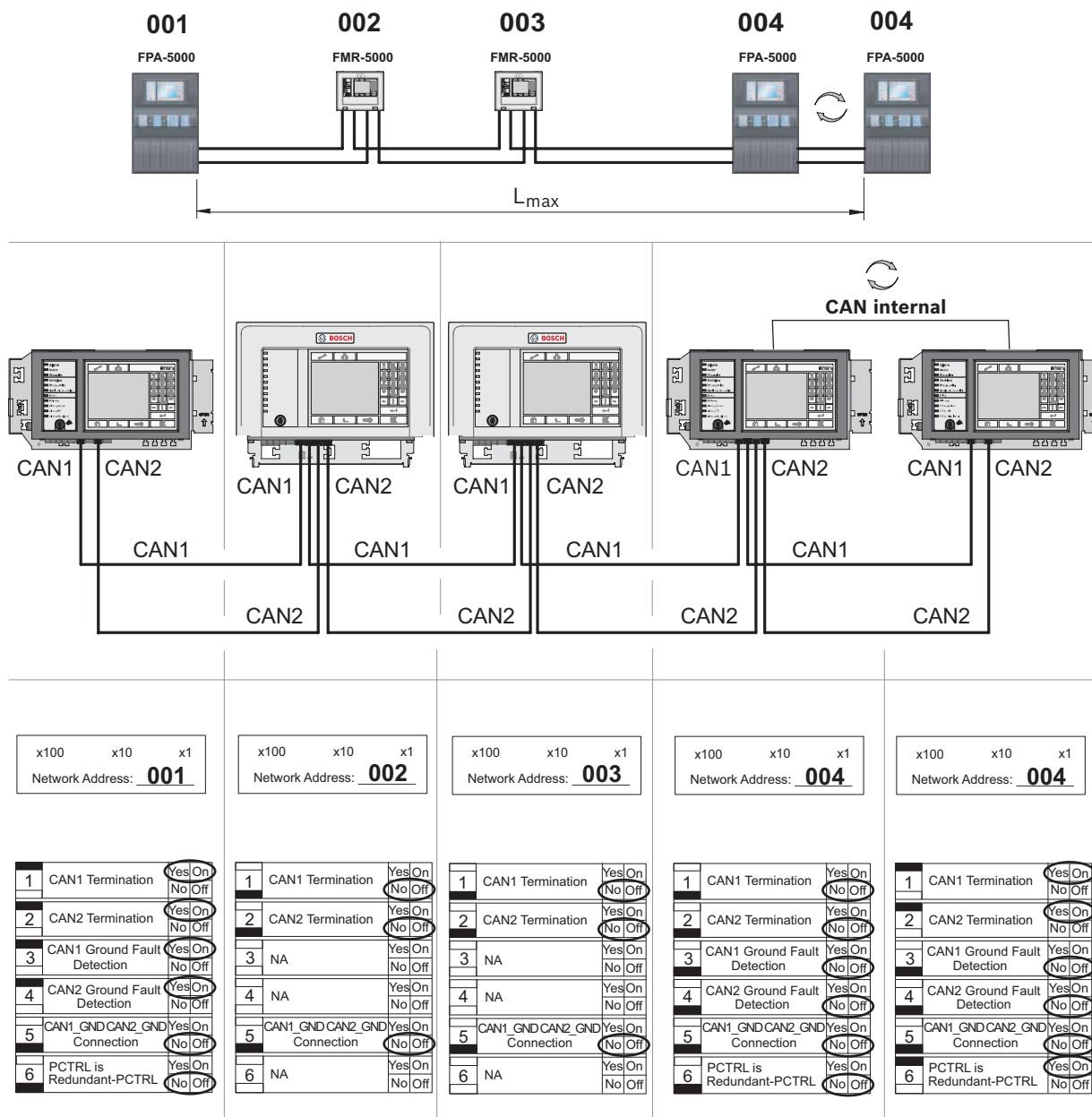
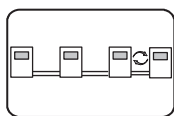


Rysunek 7.16: Topologia magistrali z centralą nadmiarową



Rysunek 7.17: Topologia magistrali z siecią nadmiarową

Magistrala z siecią nadmiarową i centralą nadmiarową FPA-5000



Rysunek 7.18: Topologia magistrali z siecią nadmiarową i centralą nadmiarową

8 Połączenia

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

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

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

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

Należy pamiętać o minimalnym promieniu zgięcia określonym w specyfikacji kabla.



8.1 Okablowanie kontrolera centrali

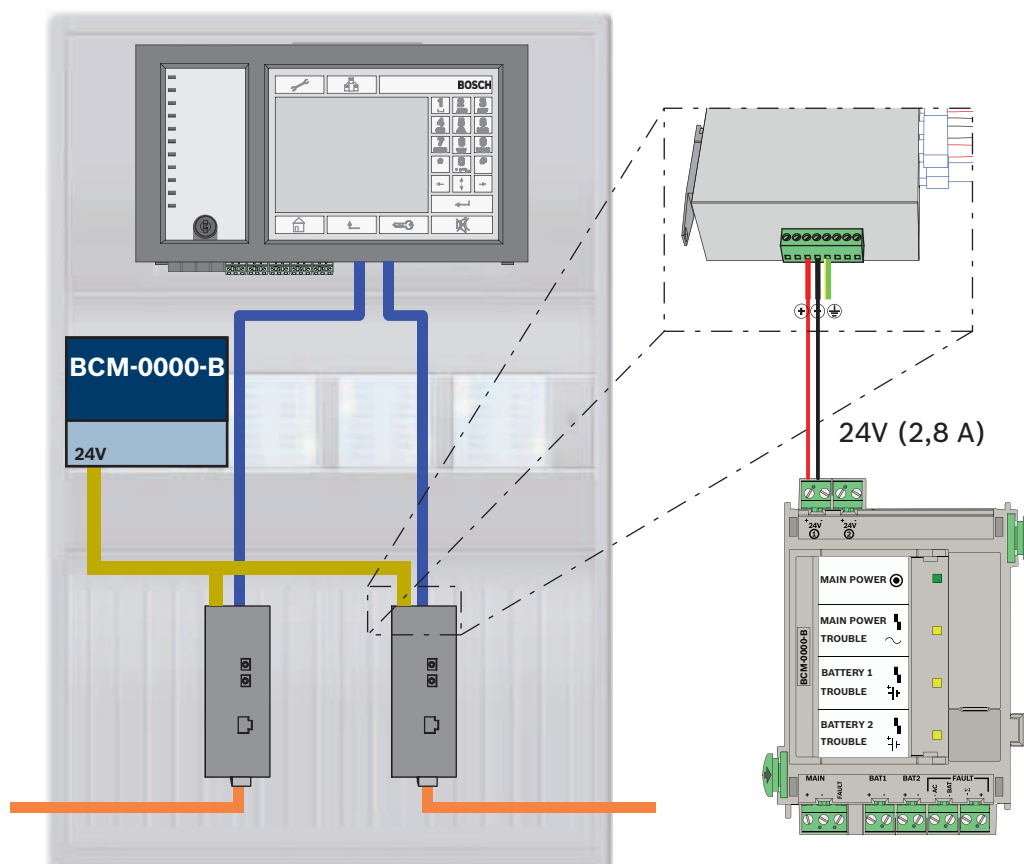
8.1.1 Konwertery transmisji i zasilanie

Połączenie konwerterów transmisji

Uwaga!

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





Rysunek 8.1: Podłączenie konwertera transmisji do zasilania i kontrolera centrali

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

8.2

Przełącznik z zasilaniem i przekaźnikiem usterki



Uwaga!

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

Połączenie przełącznika

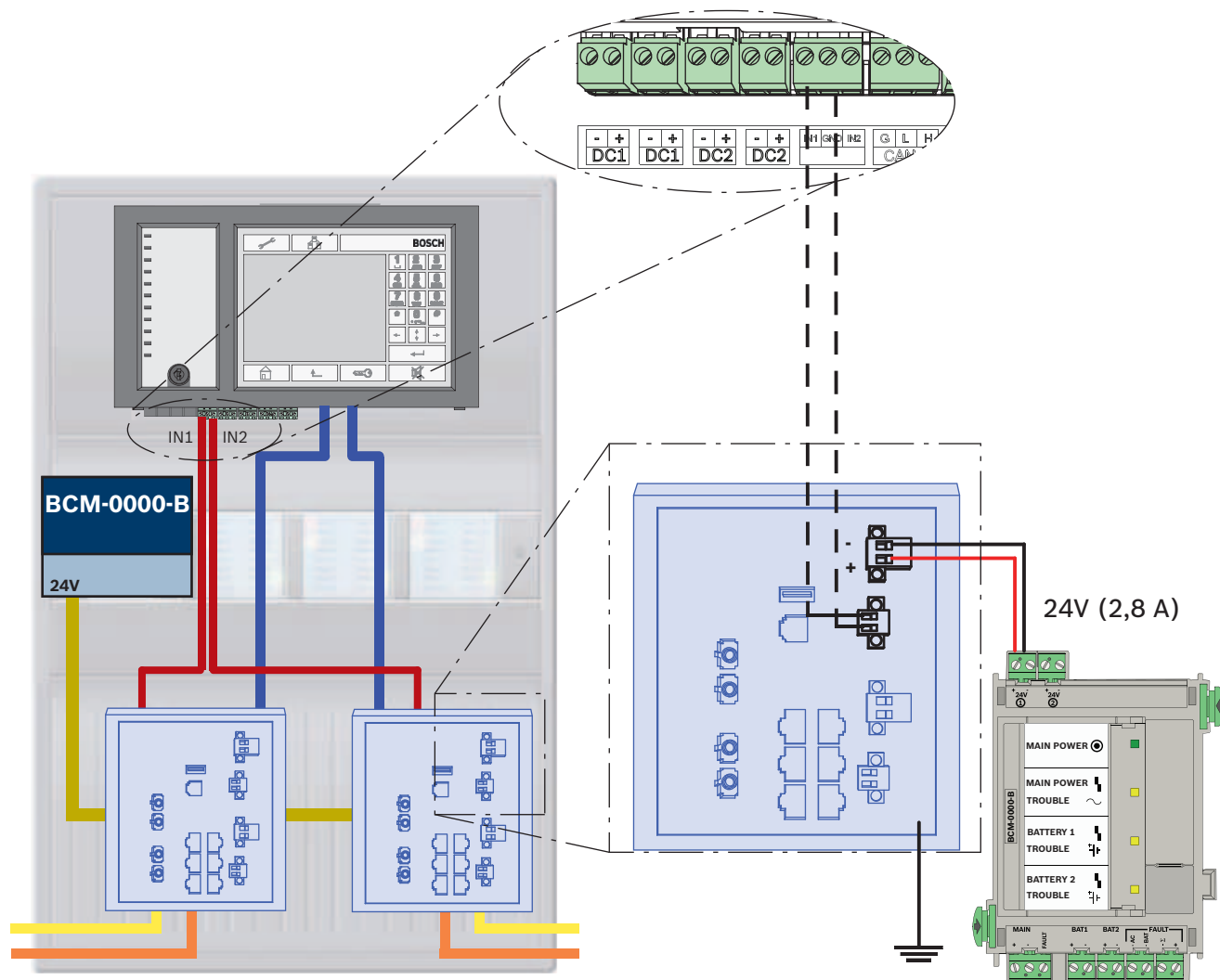
Wyjścia sygnału usterki przełączników można podłączyć do wejść kontrolera centrali MPC lub modułu wejścia i wyjścia IOP.

**Uwaga!**

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

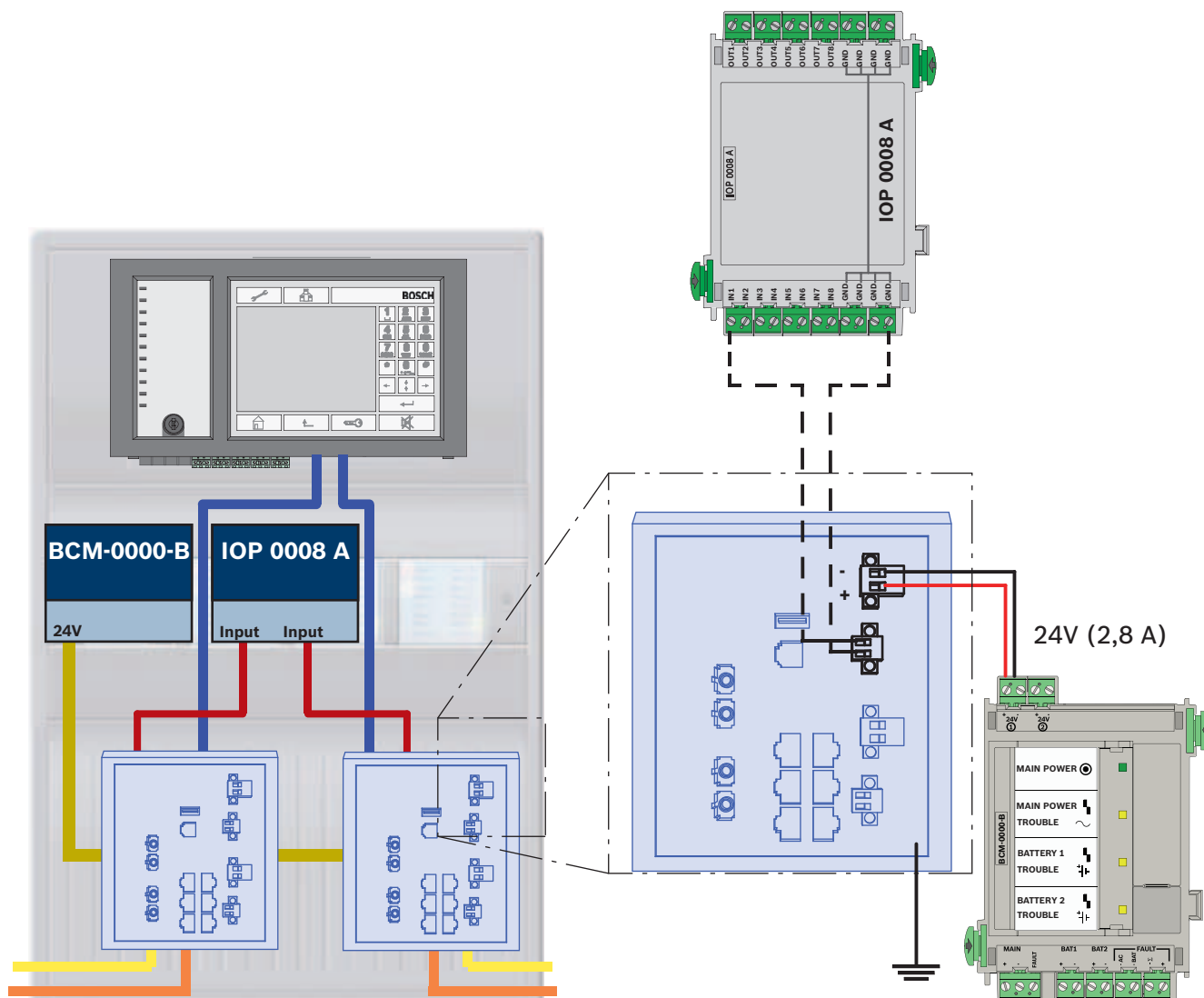
Istnieje połączenie pomiędzy dwoma przełącznikami. Jest to możliwe, np. w przypadku sieci szkieletowej z podpętlami.

Zasilanie przełącznika jest zaprojektowane nadmiarowo.

Podłączenie przełączników z raportowaniem usterek do wejść MPC.

Rysunek 8.2: Podłączenie przełącznika transmisji do zasilania i kontrolera centrali

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

Podłączenie przełączników z raportowaniem usterek do wejść modułu IOP:**Rysunek 8.3: Podłączenie przełącznika do zasilania i modułu IOP**

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

8.3**Okablowanie modułu zdalnego sterowania FMR-5000**

Moduł zdalnego sterowania musi być zasilany za pośrednictwem zewnętrznego zasilacza FPP-5000. Podłączenie do sieci jest tworzone przy użyciu dwóch konwerterów transmisji w PSS 0002 A lub USF 0000 A.

**Uwaga!**

Należy pamiętać, że zgodnie z normą EN 54-13, zasilacz zewnętrzny FPP-5000 i PSF 0002 A (PSS 0002 A) muszą być zainstalowane w bezpośrednim sąsiedztwie (bez wolnej przestrzeni) modułu zdalnego sterowania FMR-xxxx. Należy wykluczyć możliwość dotknięcia kabli łączących składniki, ponieważ nie są one monitorowane zgodnie z normą EN 54-13.

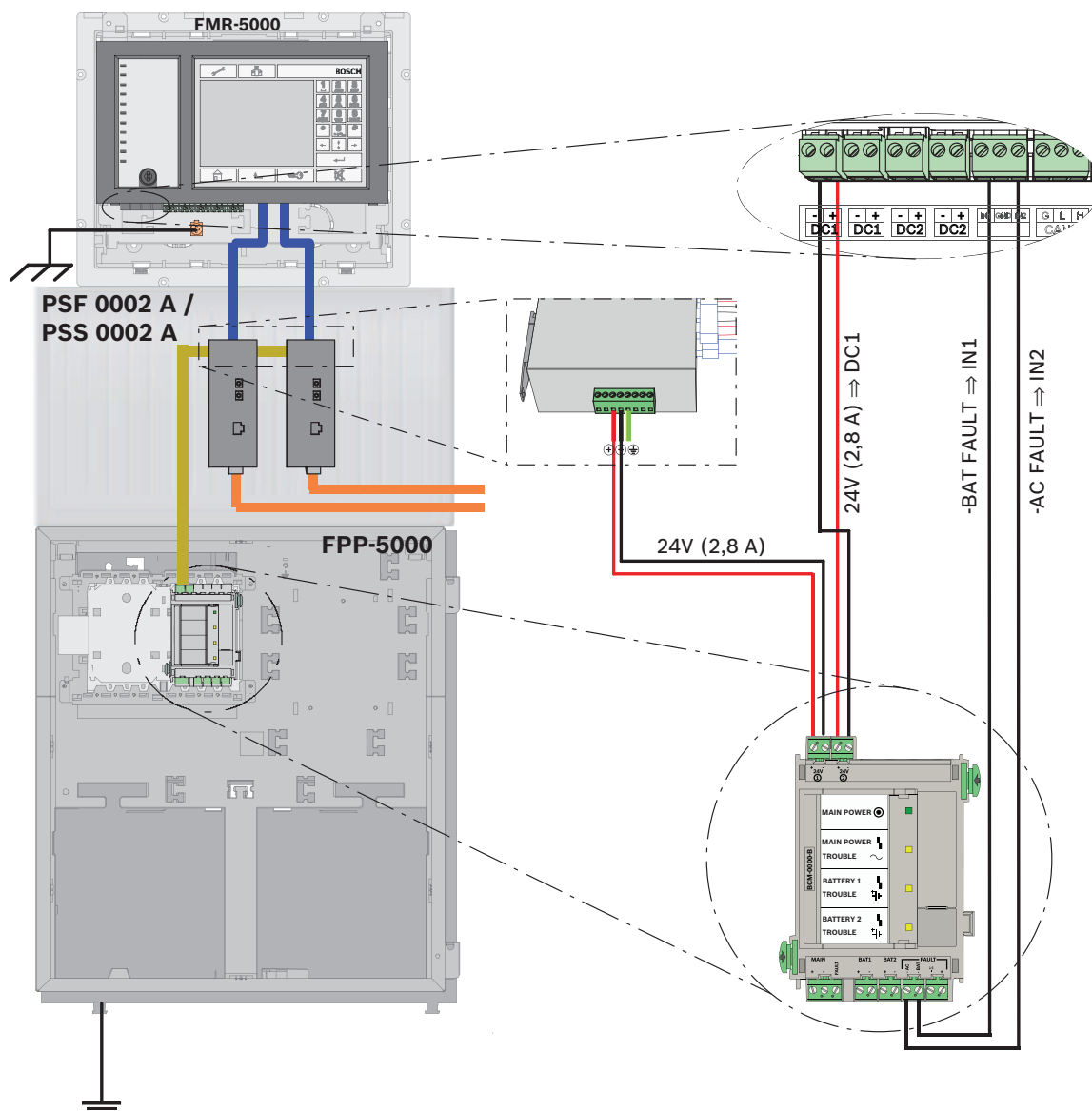
**Uwaga!**

Do podłączenia modułu zdalnego sterowania FMR-5000 do sieci central Ethernet należy używać wyłącznie konwerterów transmisji.

W przypadku modułu zdalnego sterowania niedozwolone jest użycie przełączników.

**Uwaga!**

Zawsze podczas podłączania modułu zdalnego sterowania FMR-5000 do sieci central Ethernet musi działać jego uziemienie.



Rysunek 8.4: Okablowanie modułu zdalnego sterowania

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

9

Załącznik

9.1

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 dwie 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 nadmiarowości (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	8
Adresowanie	51
Przełącznik obrotowy	51

D

Dźwiękowy system alarmowy	25, 33
---------------------------	--------

I

Interfejs CAN	31, 50
Interfejs Ethernet	50
Interfejs RS232	50
Interfejs USB	50

K

Kable światłowodowe	
EKS	31
Kontroler centrali	
System sieciowy	50

L

LLDP	8
------	---

N

Nadmiarowe	51
Nadmiarowość	
Adresowanie	51
Numer przełącznika obrotowego (RSN)	51

P

Parametry	
RSTP;RSTP:Parametry	14
PAVIRO	11, 25, 33
Pojemność sieci	8
Połączenie z siecią	31, 51
Długość kabla	31
Topologia magistrali	51
Topologia pętli	31, 51
Połączenie z siecią poprzez CAN	11
Połączenie z siecią poprzez TCP/IP	11
Praesideo	11, 25, 33
Przełącznik obrotowy	51
Przełączniki DIP	51

R

Remote Alert	30
Remote Connect	25, 33
Remote Maintenance	27
dla Remote Portal	29
dla sieci Private Secure Network	29
Remote Portal	29, 35

Remote Services	25, 33, 35
Licencja	37
Nawiązywanie połączenia zdalnego	37
Podłączanie bezpiecznej bramy sieciowej Secure	
Network Gateway	36
Ponowne zamawianie licencji	37
Przypisywanie licencji	37
Rozdzielanie podsieci	36
Tworzenie konta Remote Portal	35
RSTP	8

S

Secure Network Gateway	25, 33, 36
Serwer OPC	11, 50
Sieć	
Adresowanie	54
Kabel	32
Kabel światłowodowy	31
Ograniczenia;Ograniczenia:Sieć	31
Sieć CAN	11
Sieć Ethernet	11
Sieć: kontroler centrali	50
Sieć: Okablowanie	32

T

Topologia magistrali	51
Topologia pętli	51
Topologia: Magistrala	51
Topologia: Pętla	51
Topologie Ethernet	12
Topologie, Ethernet	12

U

Usługi	11
Ustawienia standardowe, Ethernet;Ethernet,	
ustawienia standardowe	13

Bosch Sicherheitssysteme GmbH

Robert-Bosch-Ring 5

85630 Grasbrunn

Germany

www.boschsecurity.com

© Bosch Sicherheitssysteme GmbH, 2017