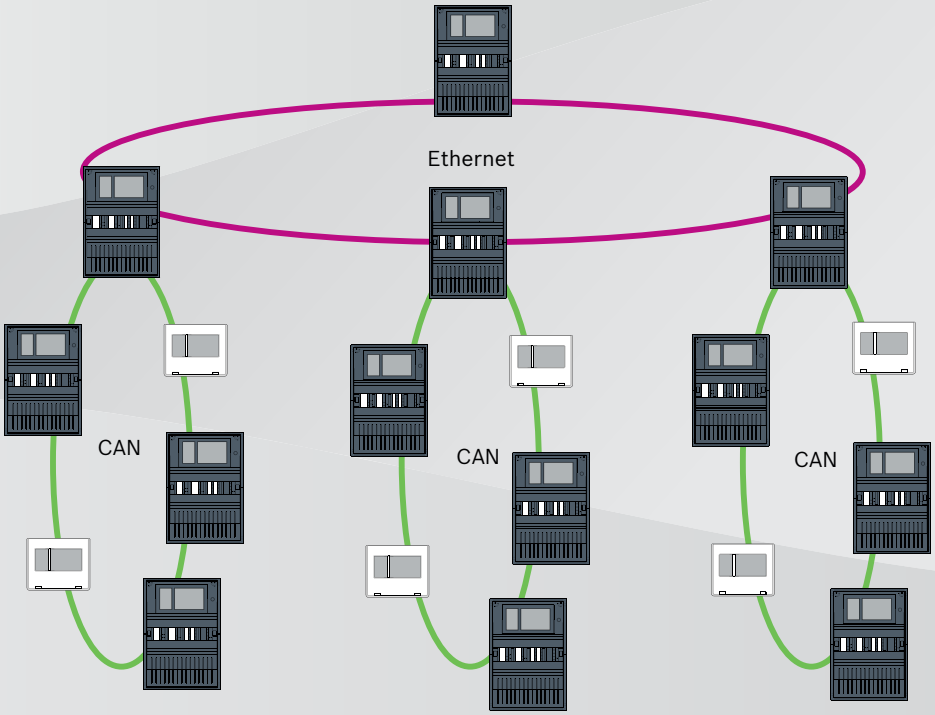
AVENAR panel series | FPA-5000 | FPA-1200



es Networking manual

Contenido

1 Seguridad

En este capítulo encontrará medidas organizativas para el PC donde se ejecuten clientes de servicio para la gama Bosch de productos antiincendios. Está obligado a cumplir estos acuerdos contractuales.
Encontrará también avisos de seguridad recopilados y ordenados por temas. Más adelante, los avisos de seguridad se colocan antes de la instrucción relacionada.

1.1 Medidas organizativas para el PC donde se ejecuten clientes de servicio

Introducción

La gama Bosch de productos antiincendios cubre los programas de PC (clientes de servicio) que se ejecutan en un ordenador, lo que requiere una conexión física con el sistema de detección de incendios. Por razones de seguridad y según los requisitos normativos estándar, el sistema de detección de incendios no se debe instalar en una red compartida. Esto a su vez significa que toda la red del sistema de detección de incendios y el PC donde se ejecuta el cliente de servicios deben crear una red dedicada físicamente. Como Bosch solo desarrolla los clientes de servicio, pero no los PC en los que se ejecutan, Bosch no puede controlar el ordenador. Para reducir el riesgo de posibles problemas de seguridad en este documento se definen medidas organizativas.

Medidas

Si las medidas que se describen a continuación requieren una conexión a Internet - o el cliente de servicio requiere una conexión temporal a Internet para licencias, el PC debe estar físicamente aislado de la red del sistema de detección de incendios antes de conectar el PC a Internet. La conexión a Internet deberá eliminarse antes de volver a conectar el PC a la red del sistema de detección de incendios de nuevo.

1. Sistemas operativos
   Bosch documenta los requisitos previos para los clientes de servicio, incluidas las versiones de sistema operativo. Se garantiza que los clientes son compatibles con estas versiones. El sistema operativo en el que se ejecuta el cliente debe actualizarse periódicamente para corregir posibles vulnerabilidades de seguridad.
   El sistema debe estar configurado de forma que solo permita el acceso de escritura a estas las carpetas, que son necesarias para la tarea correspondiente. De forma predeterminada, a todos los usuarios se les concederá permisos de solo lectura.
2. Antivirus
   En el ordenador debe estar instalado y en ejecución un software antivirus de última generación. Sus archivos de definición deben actualizarse periódicamente.
3. Firewall
   En el PC debe estar instalado y en ejecución un cortafuegos de software. Debe configurarse de forma que permita el tráfico entre el cliente de servicio y el sistema de detección de incendios, actualizaciones para el sistema operativo y el software antivirus. Además, debe bloquear el resto del tráfico.
4. Inicio de sesión de usuario segura
   El acceso al PC debe limitarse a los operadores que utilizan el cliente de servicio instalado. El inicio de sesión debe estar protegido por medios de última generación. Si se elige una contraseña para proteger el acceso, las políticas impondrán reglas de contraseña de última generación.
   La regla de las dos personas (el principio de los cuatro ojos) o la autenticación multifactor son los métodos que se recomiendan para reforzar la autenticación si procede.

5. Software y servicios
   La cantidad de software instalado en el PC se reducirá al mínimo. Se instalará únicamente el software que requiera el cliente de servicio y el software para las tareas correspondientes.
6. Limitación de uso
   El uso del PC debe estar restringido a las tareas relacionadas con el servicio mediante recursos organizativos. Esto incluye también el uso de Internet para otros fines distintos a los que se describen en este documento.
7. Separación de funciones
   Las funciones y áreas de responsabilidad se separarán para reducir las posibilidades de modificación no autorizada o no intencionada o el uso indebido, es decir, se asignarán tareas distintas a los distintos roles.
8. Supervisión
   Todos los intentos de acceso al PC que ejecuta el cliente del servicio se deben supervisar para reconocer el acceso no autorizado al PC y a Internet.

1.2 Explicación de los símbolos de seguridad

Advertencia!
Indica una situación peligrosa que, si no se evita, podría resultar en lesiones graves o incluso la muerte.

Precaución!
Indica una situación peligrosa que, si no se evita, podría resultar en lesiones leves o moderadas.

Aviso!
Indica una situación que, si no se evita, podría provocar daños en el equipo, en el entorno, o bien pérdida de datos.

1.3 Notificaciones de seguridad

Conversor de medios

Advertencia!
Luz láser
No mire directamente al haz de luz a simple vista ni a través de instrumentos visuales de ningún tipo (p. ej., una lupa o microscopio). El incumplimiento de este aviso supone un peligro para los ojos a una distancia inferior a 100 mm. La luz procede de los terminales visuales o del extremo de los cables de fibra óptica conectados a ellos. Diodo láser de CLASE 2M, longitud de onda 650 nm, salida <2 mW, de acuerdo con IEC 60825-1.

Remote Services

Precaución!
Para el acceso por internet utilice únicamente BoschRemote Services.

Precaución!
Los Remote Services requieren una conexión IP segura. Se requiere BoschRemote Services o conexión con Private Secure Network.
Con Private Secure Network se proporciona una red IP basada en DSL con un acceso inalámbrico opcional en el lado de la central (EffiLink). Remote Services para Private Secure Network solo está disponible en Alemania con un acuerdo de servicios con Bosch BT-IE.

Aviso!
Se requiere una red Ethernet exclusiva para configurar una red de centrales de alarma de incendio.
Utilizar un sistema de detección de incendios en cualquier otra red Ethernet se hace a cuenta y riesgo del usuario. Bosch rechaza toda responsabilidad o garantía que derive de esta aplicación incorrecta.
En el caso de una red Ethernet no exclusiva, no se pueden garantizar la transmisión fiable de alarmas ni la seguridad de las TI.

Red de centrales

Aviso!
EN 54
Para garantizar que la red se configura conforme a la normativa EN 54, use solo componentes aprobados para su uso en redes de alarmas de incendio centrales.
Los conmutadores RSTP externos y los conversores de medios de las redes Ethernet deben ir instalados en las carcasas de las centrales. La instalación fuera de la carcasa de una central no cumple la normativa EN 54.

Aviso!
Longitud del cable TX
Todas las conexiones IP deben ser directas o a través de conversores de medios aprobados por Bosch. La longitud de cable TX entre nodos debe ser inferior a 100 m.

Aviso!
VdS 2540
Para cumplir los requisitos de VdS 2540 para las rutas de transmisión de datos utilice cable de fibra óptica para las conexiones Ethernet. Para las conexiones dentro de una carcasa, es posible usar cables Ethernet TX.

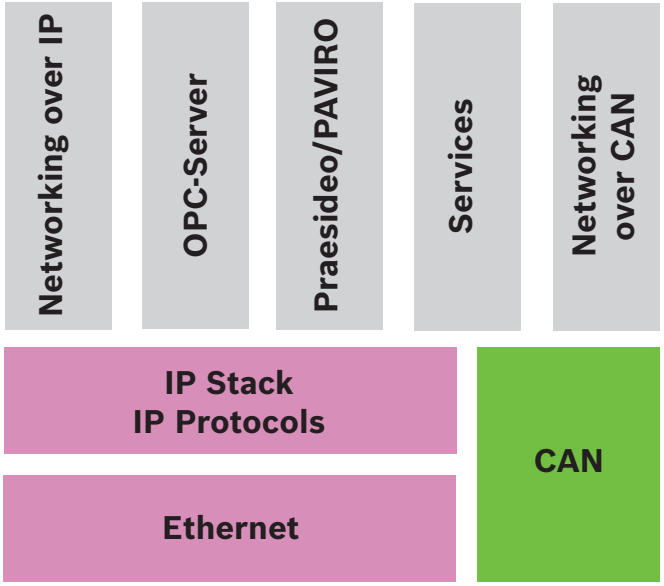
Aviso!
En las aplicaciones estándar, utilice configuraciones de red estándar.
Solo los usuarios con experiencia pueden cambiar los ajustes de red estándar, siempre que tengan el conocimiento adecuado en redes.

Aviso!
Topologías aplicables
La funcionalidad y la comunicación entre centrales está limitada por el tipo de central. Consulte las especificaciones de la central para obtener información sobre los servicios, el número de centrales conectables y el número de teclados remotos conectables.

2 Introducción

Este documento está dirigido a lectores con experiencia en diseño e instalación de sistemas de detección de incendios que cumplen la norma EN 54. Además, se necesitan conocimientos de redes.
Este documento describe diversas topologías de red de alarmas de incendio. Las topologías se describen independiente del tipo de central de incendio.
Para crear redes de centrales correspondientes a las topologías presentadas y a los servicios de conexión, es necesario el patrón de funcionamiento en red descrito en este documento.
El documento proporciona una descripción general de las condiciones básicas, los valores límite y los procedimientos generales para la instalación y diseño de redes de centrales.
Las descripciones detalladas de la instalación de los componentes individuales se encuentran en las respectivas guías de instalación.
La descripción del módulo de interfaz de usuario del controlador de la central se encuentra en la guía del usuario incluida con el dispositivo.
La interfaz de usuario del software de programación FSP-5000-RPS se describe en la ayuda en línea.

3 Descripción del sistema



En la red, se utilizan los protocolos de interfaz Ethernet e IP para distintos servicios. El módulo de interfaz Ethernet se puede desactivar por completo o se puede desactivar su utilización para funcionamiento en red mediante TCP/IP. Esta deshabilitación puede resultar necesaria para el funcionamiento en red a través de CAN.

Activación de servicios

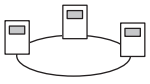
- funcionamiento en red por TCP/IP
  En FSP-5000-RPS, active la comunicación entre centrales en la red Ethernet
- Servidores OPC
  Añada un servidor OPC a la configuración de FSP-5000-RPS
- Conexión Praesideo/PAVIRO
  Añada un sistema de alarma por voz a la configuración de FSP-5000-RPS y configure los activadores virtuales.
- Remote Services (Remote Connect como requisito previo Remote Maintenance y Remote Alert)
  Active la casilla de verificación correspondiente en FSP-5000-RPS

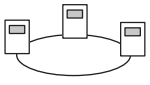
– Remote Services (Remote Connect como requisito previo Remote Maintenance y Remote Alert) para Private Secure Network
  Añada acceso remoto a la configuración de FSP-5000-RPS y configure el acceso remoto en FSP-5000-RPS.

Aviso!
Transferencia de datos accidental
Si el módulo Ethernet del controlador de la central se va a usar solo para la comunicación con un servidor OPC o para Remote Services, deshabilite la comunicación de la central a través de TCP/IP en FSP-5000-RPS. De lo contrario, los datos del incendio podrían transferirse accidentalmente a través de Ethernet.

Para usar los servicios basados en TCP/IP o Ethernet, es necesario activar las interfaces Ethernet y se deben configurar TCP/IP correctamente.

Red de centrales y teclados remotos
En la siguiente tabla se muestran las opciones para el funcionamiento de centrales/teclados remotos en red en función de la topología de red y del tipo de central. Tenga en cuenta los límites determinados por la topología de red.

Topología	**AVENAR panel 8000, licencia Premium.**	**AVENAR panel 8000, licencia estándar.**	**AVENAR panel 2000, licencia Premium.**	**AVENAR panel 2000, licencia estándar.**
 Independiente	Posible	Posible	Posible	Posible
 Lazo	Máximo 32 centrales/ teclados remotos, conectividad con AVENAR panel 2000, licencia Premium y FPA	Máximo 32 centrales/ teclados remotos, conectividad con AVENAR panel 2000, licencia Premium y FPA	Máximo 32 centrales/ teclados remotos, conectividad con AVENAR panel 8000 y FPA	1 central y un máximo de 3 teclados remotos
 Redundancia de centrales	El controlador de central redundante también debe ser Premium. También se puede usar un teclado remoto como central redundante.	El controlador de la central redundante puede ser estándar. También se puede usar un teclado remoto como central redundante.	Imposible	Imposible

Topología	**FPA-5000**	**FPA-1200**
 Independiente	Posible	Posible
 Lazo	Máx. de centrales y teclados remotos 32	1 central y un máximo de 3 teclados remotos

Topología	FPA-5000	FPA-1200
Redundancia de centrales	Posible	No es posible (el DIP 6 del controlador de la central no es funcional).

Para ampliar una red de FPA-5000, Bosch recomienda hacerlo con una central de la serie AVENAR panel.
Al intercambiar una central de la serie FPA con una de la serie AVENAR panel, basta con intercambiar solo el controlador de la central. Recuerde que las centrales de la serie AVENAR panel no admiten tarjetas de direcciones. Si se usa un conmutador Ethernet conectado, es posible continuar usándolo.
Al intercambiar un teclado remoto de la serie FPA por otro de la serie AVENAR panel, compruebe que la resistencia de la línea esté dentro del rango especificado para el teclado remoto de la serie AVENAR panel.

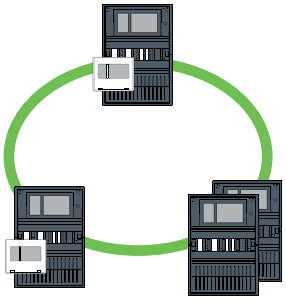
Aviso!
Instalación del firmware
Las centrales conectadas deben tener la misma versión de firmware.
La instalación del firmware solo es posible para la central activa. Para centrales redundantes realice la instalación de firmware en ambas centrales. Para ello, tiene que cambiar los roles de las centrales y volver a cambiarlos de nuevo tras la correcta instalación del firmware.

Aviso!
Controlador de central redundante
No es posible combinar un controlador de central de la serie AVENAR panel con un controlador de central de la serie FPA para aportar redundancia.

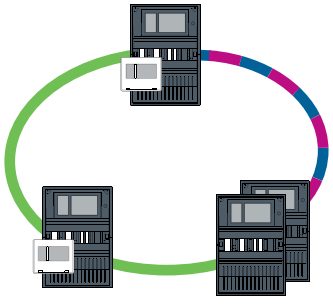
4 Topologías

Este documento describe diversas topologías de red de alarmas de incendio. Las topologías se describen independiente del tipo de central de incendio.

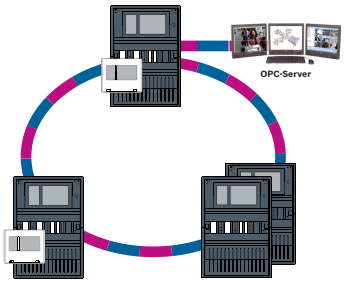
Aviso!
Topologías aplicables
La funcionalidad y la comunicación entre centrales está limitada por el tipo de central.
Consulte las especificaciones de la central para obtener información sobre los servicios, el número de centrales conectables y el número de teclados remotos conectables.



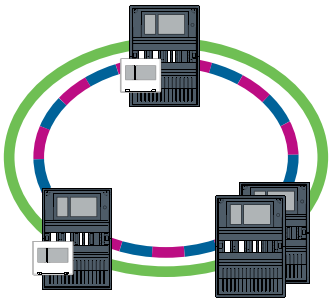
Lazo CAN, Página 15



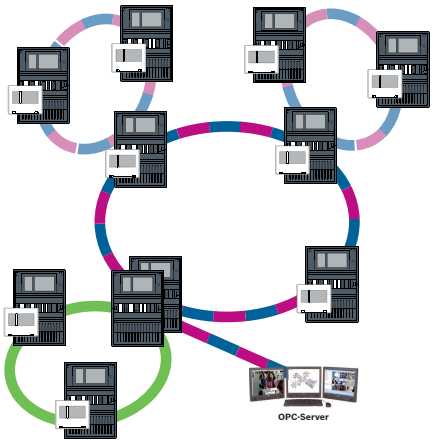
Bucle CAN con segmentos Ethernet, Página 17



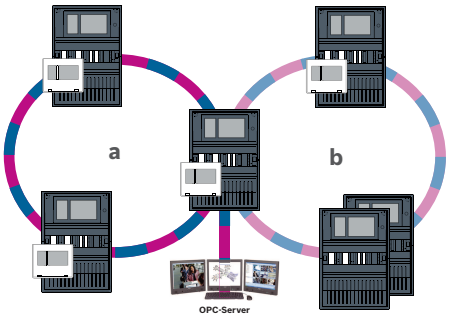
Lazo Ethernet, Página 15
Lazo Ethernet con servidor OPC, Página 16
Lazo Ethernet con servidor OPC a una central redundante, Página 16



Lazo doble Ethernet/CAN, Página 17

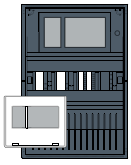
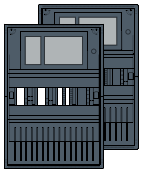


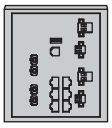
Red troncal Ethernet con sublazos (Ethernet/CAN), Página 17



Conexión de lazos Ethernet, Página 19

Cable	Descripción
	Cable Ethernet TX (cobre), longitud de cable TX entre nodos <100 m
	Cable Ethernet FX (cable de fibra óptica)
	Cable Ethernet TX o FX, longitud de cable TX entre nodos <100 m
	Cable de CAN, longitud del cable de CAN de nodo a nodo <1000 m

Dispositivo	Descripción
	Central o teclado remoto (en la topología Ethernet un conmutador RSTP interno cada uno)
	Central redundante (en la topología Ethernet un conmutador RSTP interno) Es posible utilizar un teclado remoto como controlador de central redundante. Las conexiones de red y los ajustes son idénticos para un controlador de central redundante y para un teclado redundante. El uso de un teclado redundante solo es aplicable a AVENAR panel 8000.

Dispositivo	Descripción
	Conmutador Ethernet como conmutador RSTP externo (en general, conmutador Ethernet MM)
	Conversor de medios
	Puerta de acceso a red segura para Remote Services

Límites en la red

El número de centrales y de teclados remotos que se pueden conectar en red depende de la topología de red elegida.

Las centrales y los teclados remotos conectados en red se conocen como nodos.

- El número máximo de puntos de detección de una red es de 32768.
- El número máximo de puntos de detección por central que se pueden usar en una red es de 2048.
- El número de nodos por sistema depende del tipo de topología.
  Un nodo puede ser un controlador de central o un teclado remoto.
- El número máximo de nodos en una topología de lazo es de 32.
- Con FSP-5000-RPS, es posible asignar hasta 3 teclados remotos configurados a una central.

El cableado entre los nodos y la longitud de cable máxima permitida también se determina en función de la topología elegida.

Se puede combinar un máximo de 32 controladores de central, teclados remotos y servidores OPC para formar una red.

En función del uso para el que esté destinado, los controladores de central y los teclados remotos se pueden dividir en grupos y definirse como nodos de red o nodos locales. Por norma general, dentro un grupo determinado, solo se puede visualizar el estado de los paneles de control del grupo definido. El estado de todos los paneles de control se puede mostrar y/o procesar desde los nodos de red, independientemente del grupo al que pertenezcan las centrales.

Dirección de nodo físico

Para identificar una central o un teclado remoto en la red, se utiliza una dirección única, conocida como dirección del nodo físico.

Aviso!

Dirección del nodo físico para centrales redundantes

Una central redundante debe tener la misma dirección del nodo físico que la central principal asignada.

Aviso!

La red que se utilice debe cumplir los siguientes requisitos mínimos:

Capacidad mínima de proceso: 1 Mbps

Latencia máxima: 250 ms

Aviso!
EN 54
Para garantizar que la red se configura conforme a la normativa EN 54, use solo componentes aprobados para su uso en redes de alarmas de incendio centrales.
Los conmutadores RSTP externos y los conversores de medios de las redes Ethernet deben ir instalados en las carcasas de las centrales. La instalación fuera de la carcasa de una central no cumple la normativa EN 54.

Aviso!
Central redundante: EN 54-2
Según la normativa EN 54-2, es posible conectar 512 puntos de detección como máximo por central. Si se supera este número, es necesario diseñar la central de manera redundante. Asimismo, si una central actúa como una interfaz con un sublazo CAN y se conectan más de 512 puntos de detección en el sublazo, tendrá que diseñar la central de manera redundante. El conmutador RSTP que conecta 2 lazos realiza la redundancia.
Para una central independiente puede conectar un máximo de 4096 puntos de detección, incluso aunque se haya diseñado de manera redundante. Si la central está incluida en una red, es posible conectar 2048 puntos de detección como máximo.

Aviso!
Asegúrese de que la dirección de nodo físico asignada a la central coincida con la del software de programación, que es el responsable de configurar el último número de la dirección IP en los ajustes estándar.
Active RSTP como protocolo de redundancia y acepte los valores estándar predeterminados.

Ajustes Ethernet estándar de la central de incendio
En los ajustes estándar de la central de incendio, tanto el software de programación FSP-5000-RPS como la unidad de control utilizan la dirección del nodo físico configurada como el último número de la dirección IP.

Aviso!
Es necesario configurar correctamente la dirección del nodo físico en los controladores de la central y en el software de programación FSP-5000-RPS para que la red funcione adecuadamente.

Aviso!
El uso de la redundancia Ethernet se debe activar por separado en el controlador de la central.

- Ajustes IP
  - Dirección IP 192.168.1.x
    El último dígito de la dirección IP de los ajustes estándar coincide siempre con la dirección del nodo físico establecida en el controlador de la central.
  - Máscara de red 255.255.255.0
  - Puerta de acceso 192.168.1.254
  - Dirección multicast 239.192.0.1
  - Número de puerto 25001 - 25008 (solo se puede configurar el primer puerto; siempre se utilizan 8 puertos consecutivos)
- Parámetros RSTP (ajustes por defecto)
  - Bridge Priority 32768

- Hello Time 2
- Max. Age 20
- Forward Delay 15

Aviso!
Puede usar los ajustes estándar de la configuración IP con redes de hasta 20 conmutadores RSTP.
En las redes con más de 20 conmutadores RSTP, se requieren ajustes adicionales en función de la topología. Para ello, se requiere un conocimiento exhaustivo sobre redes.

Ajustes para lazos con más de 20 conmutadores RSTP
Si hay más de 20 conmutadores RSTP en la red, modifique los ajustes de RSTP en el controlador de la central y en el software de programación. Los controladores de central, los teclados remotos y los conmutadores RSTP externos conectados se consideran conmutadores RSTP. Los controladores de central redundantes no se consideran conmutadores RSTP porque el conmutador que incluyen no funciona como un conmutador RSTP.

- Parámetros de RSTP
  - Mantener Bridge Priority32768
  - Mantener Hello Time2
  - Cambiar Max. Age de 20 a 40
  - Cambiar Forward Delay de 15 a 25

Parámetros
- Se puede usar un máximo de 32 nodos en un lazo.
- El diámetro de red no debe ser mayor de 32, consulte *Diámetro de red, Página 22*.
- Los conmutador Ethernet no deben utilizarse fuera de las carcasas de la central.
- Los conversores de soportes no deben utilizarse fuera de las carcasas de la central.

Características
- La red cumple la normativa EN 54.
- La red utiliza RSTP.

Conexión a BIS con servidor OPC
Al conectar un sistema de gestión de edificios (BIS) a través de un servidor OPC y Ethernet 100BaseTX en varias redes de edificios, debe acordar con el administrador de la red lo siguiente:

1. ¿Se ha diseñado la red para conexiones destinadas a varias ubicaciones? (p. ej. no debe haber interferencias técnicas debido a diferencias en la tensión de derivación a tierra)
2. ¿Es el ancho de banda de los usuarios de bus suficiente para la red?

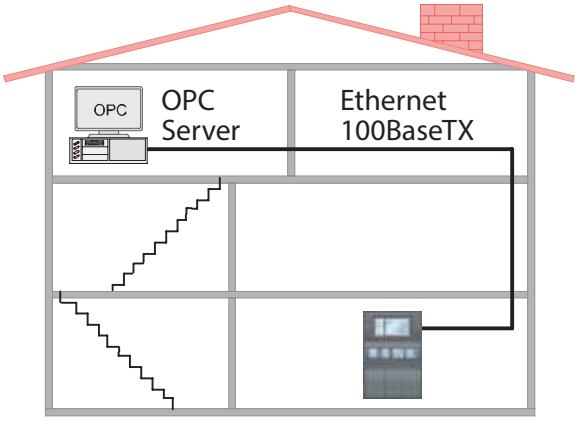


Figura 4.1: Conexión a BIS a través de un servidor OPC

Información adicional al usar un servidor OPC

Es necesario añadir los servidores OPC de la red al software de programación FSP-5000-RPS.

Configure los siguientes ajustes en el software FSP-5000-RPS y en el servidor OPC:

- Nodos de red
- Grupo de red
- RSN
- Dirección IP
- Puerto

El servidor OPC usa el puerto 25000 como estándar.

Aviso!

EN 54

La conexión de un sistema de gestión de edificios (p. ej., BIS) mediante una interfaz Ethernet utilizando un servidor OPC o un servidor FSI cumple con los requisitos de EN54 si la CDI realiza las funciones EN54 relevantes de forma exclusiva. Cualquier control o administración relevante para EN54 (p. ej., el control de los aparatos de notificación o la administración de la desactivación) por parte del sistema de gestión de edificios requiere una certificación EN54 específica del sistema global por parte de un organismo de certificación.

Aviso!

Software de programación FSP-5000-RPS

Debe asignar un servidor OPC a cada nodo de red cuyos estados sea necesario transmitir.

4.1 Lazo CAN

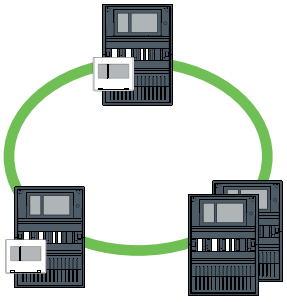


Figura 4.2: Lazo CAN

4.2 Lazo Ethernet

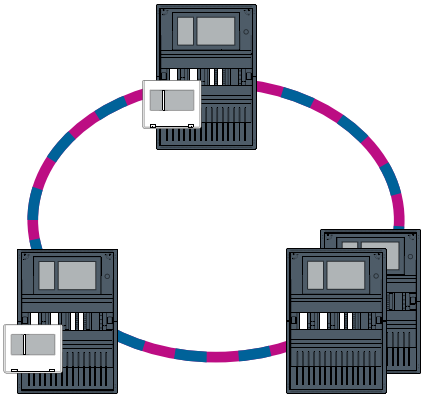


Figura 4.3: Lazo Ethernet

4.3 Lazo Ethernet con servidor OPC

El switch Ethernet que se usa para conectar el servidor OPC se debe programar por separado

Programe la dirección IP y los ajustes de redundancia del switch Ethernet, consulte *Ajustes del conmutador, Página 45*. Como el conmutador se instala en las inmediaciones directas (sin espacio intermedio), no es necesario diseñar la fuente de alimentación de manera redundante y, por tanto, las salidas de avería no se usan.

Asegúrese de que los ajustes RSTP de los controladores de la central, en FSP-5000-RPS y en el switch Ethernet son idénticos.

El servidor OPC se debe programar por separado

Programe la dirección IP, los nodos de red, el grupo de red y RSN. Consulte la sección correspondiente en el capítulo de Instalación de la Guía de funcionamiento en red.

El servidor OPC usa el puerto 25000 como estándar.

Asegúrese de que los ajustes del software de programación FSP-5000-RPS y del servidor OPC son idénticos.

Parámetros

– El servidor OPC se puede conectar a través de un cable Ethernet (cobre) o de fibra óptica.

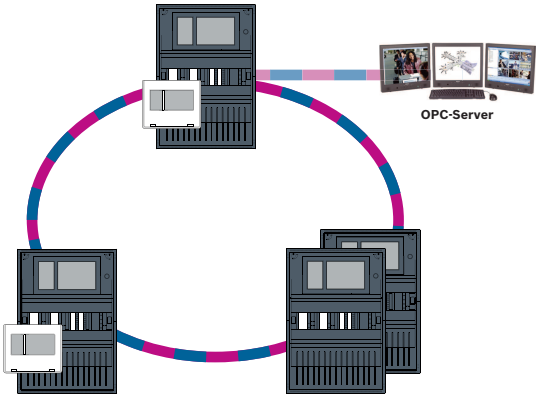


Figura 4.4: Lazo Ethernet con servidor OPC

4.4 Lazo Ethernet con servidor OPC a una central redundante

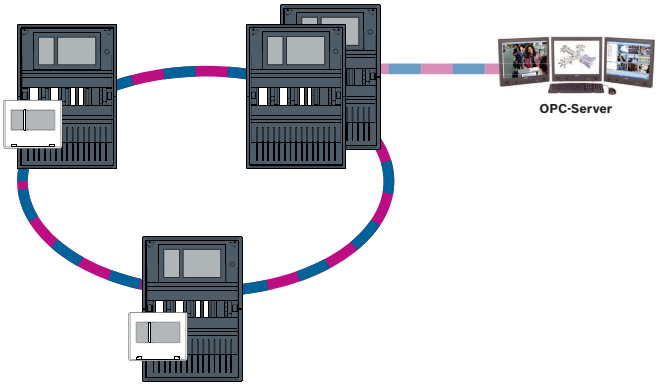


Figura 4.5: Lazo Ethernet con servidor OPC a una central redundante

4.5 Lazo doble Ethernet/CAN

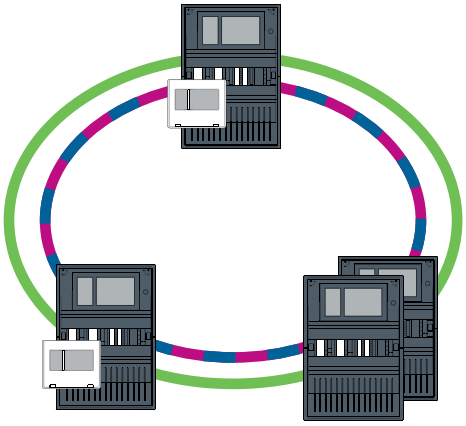


Figura 4.6: Lazo doble de Ethernet y CAN

4.6 Bucle CAN con segmentos Ethernet

La topología principal es un lazo CAN. Cuando la distancia entre dos nodos es de más de 1000 m, se puede utilizar una conexión Ethernet FX para cubrir la distancia.

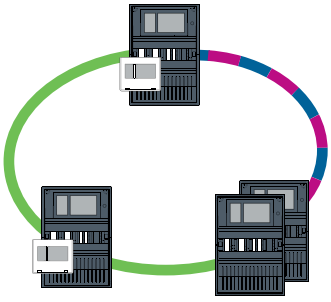


Figura 4.7: Bucle CAN con segmentos Ethernet

4.7 Red troncal Ethernet con sublazos (Ethernet/CAN)

Una red troncal Ethernet está conectada a todos los sublazos y, por tanto, un área principal de conexión con altas velocidades de transmisión de datos. De manera predeterminada, los conmutadores RSTP de la red troncal no son principales. Tenga en cuenta que con esta topología deberá determinar el diámetro de red. Los controladores de central, los teclados remotos y los conmutadores RSTP externos conectados se consideran conmutadores RSTP. Las centrales conectadas en red mediante CAN no se tienen en cuenta al determinar el diámetro de red.
Tenga en cuenta los ajustes para lazos con más de 20 conmutadores RSTP, consulte *Ajustes para lazos con más de 20 conmutadores RSTP, Página 14*.

Aviso!
Esta topología requiere realizar ajustes adicionales para todos los conmutadores RSTP de la red troncal. Por tanto, se requiere un conocimiento más exhaustivo de las redes.

Aviso!
Si la central actúa como un módulo de interfaz con sublazo CAN, dicha central también se debe diseñar de manera redundante conforme a la normativa EN 54-2 en caso de que se conecten más de 512 puntos de detección al sublazo.
Esta restricción no se aplica a los sublazos Ethernet, ya que los conmutadores que conectan los dos lazos aportan la redundancia.

Ajustes adicionales

Utilice el lazo central como red troncal. Este lazo central se debe conectar a través de Ethernet.

Aviso!

Establezca una prioridad de RSTP superior a la de los sublazos para todos los conmutadores RSTP de la red troncal. Así se garantiza que el puente raíz RSTP permanezca siempre en la red troncal, incluso en caso de avería.
Los conmutadores RSTP que conectan los lazos forman parte de la red troncal.
Utilice una prioridad RSTP de 16384 en la red troncal.

Aviso!

Cuanto más bajo sea el valor establecido, mayor será la prioridad RSTP.

Los conmutadores que se usan para conectar el servidor OPC y los sublazos se deben programar por separado

Programe la dirección IP y los ajustes de redundancia de los switch Ethernet, consulte *Ajustes del conmutador, Página 45*. En esta topología solo se deben usar las salidas de avería del conmutador si ha diseñado la fuente de alimentación para el conmutador de manera redundante o existe una conexión de conmutador a conmutador, consulte *Switch Ethernet, Página 56*.
Asegúrese de que los ajustes RSTP de los controladores de la central, en FSP-5000-RPS y en el switch Ethernet son idénticos.

Aviso!

Cambie la prioridad RSTP de los conmutadores RSTP para conectar los lazos, ya que pertenecen a la red troncal.

El servidor OPC se debe programar por separado.

Programe la dirección IP, los nodos de red, el grupo de red y RSN, consulte *Servidores OPC, Página 62*.
El servidor OPC usa el puerto 25000 como estándar.
Asegúrese de que los ajustes del software de programación RPS y del servidor OPC son idénticos.

Parámetros

– El servidor OPC se puede conectar a través de un cable Ethernet (cobre) o de fibra óptica.

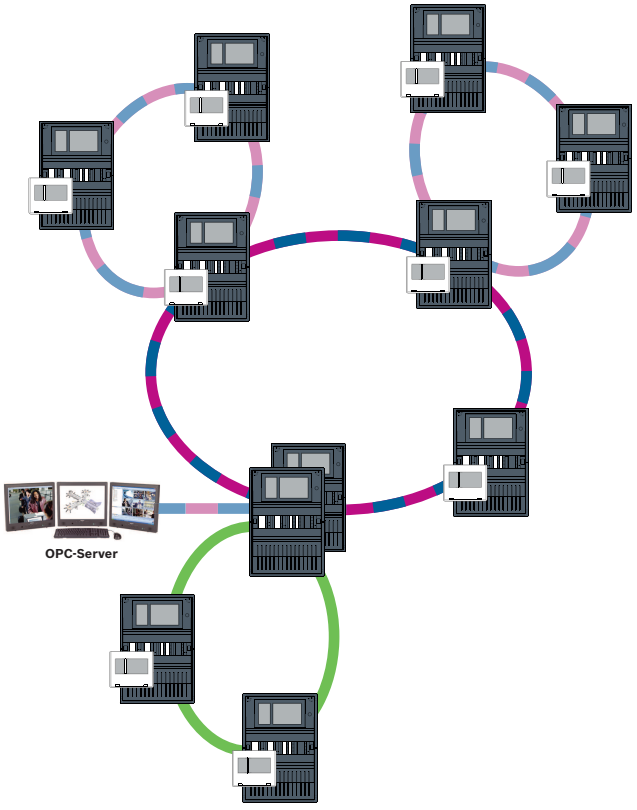


Figura 4.8: Red troncal Ethernet con sublazos

4.8 Conexión de lazos Ethernet

Aviso!
Esta topología requiere realizar ajustes adicionales para todos los conmutadores RSTP de la red troncal. Por tanto, se requiere un conocimiento más exhaustivo de las redes.

Ajustes adicionales
Esta topología es una instancia especial de la red troncal Ethernet con sublazos, consulte Red troncal Ethernet con sublazos (Ethernet/CAN). Utilice uno de los dos lazos como red troncal.

Aviso!
Para las centrales y conmutadores de la red troncal, establezca una prioridad de RSTP superior a la de los sublazos. De este modo se garantiza que el puente raíz RSTP permanezca siempre en la red troncal, incluso en caso de avería.
Los conmutadores que conectan los dos lazos forman parte de la red troncal.
Utilice una prioridad RSTP de 16384 en la red troncal.

Aviso!
Cuanto más bajo sea el valor establecido, mayor será la prioridad RSTP.

Los conmutadores que se usan para conectar el servidor OPC y el segundo lazo se deben programar por separado

Programe la dirección IP y los ajustes de redundancia del switch Ethernet, consulte *Ajustes del conmutador, Página 45*. En esta topología solo se deben usar las salidas de avería del conmutador si ha diseñado la fuente de alimentación para el conmutador de manera redundante; consulte *Switch Ethernet, Página 56*.

Asegúrese de que los ajustes RSTP de los controladores de la central, en FSP-5000-RPS y en el switch Ethernet son idénticos.

Cambie la prioridad RSTP de los conmutadores para conectar los dos lazos, ya que pertenecen a la red troncal.

El servidor OPC se debe programar por separado

Programe la dirección IP, los nodos de red, el grupo de red y RSN. Consulte la sección correspondiente en el capítulo de Instalación de la Guía de funcionamiento en red.

El servidor OPC usa el puerto 25000 como estándar.

Asegúrese de que los ajustes del software de programación FSP-5000-RPS y del servidor OPC son idénticos.

Parámetros

– El servidor OPC se puede conectar a través de un cable Ethernet (cobre) o de fibra óptica.

En estos ejemplos, el lazo a es la red troncal. El lazo b es el sublazo.

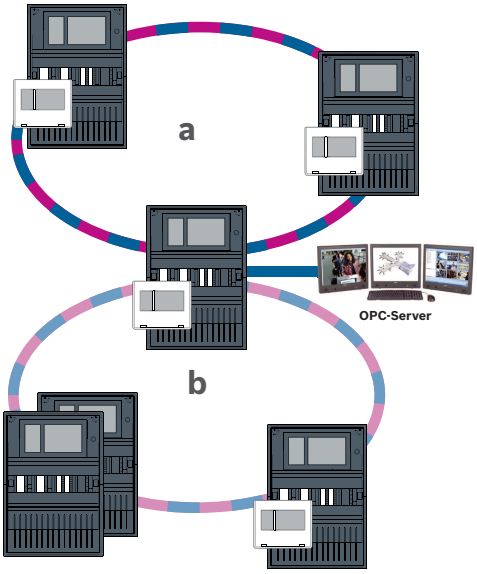


Figura 4.9: Conexión de un lazo Ethernet a través de una central no redundante

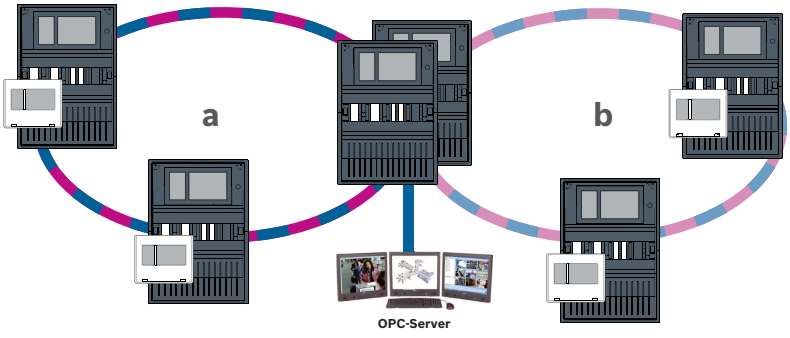


Figura 4.10: Conexión de un lazo Ethernet a través de una central redundante

5 Red Ethernet

En la red, las conexiones de red Ethernet se supervisan continuamente. Si una conexión se suspende, se detecta la interrupción. Las conexiones reparadas también se identifican. El diagnóstico de red de la central siempre muestra la dirección MAC de los hosts conectados a través de la red.

Direcciones MAC

Cada controlador de la central proporciona las siguientes direcciones MAC par la conexión de red.

– Dirección MAC para el host
– Dirección MAC para identificar el puerto ETH1
– Dirección MAC para identificar el puerto ETH2

Según el tipo de controlador de central:

– Dirección MAC para identificar el puerto ETH3
– Dirección MAC para identificar el puerto ETH4

Reglas para usar 4 puertos Ethernet

Si la central tiene 4 puertos Ethernet, aplique las reglas siguientes en el orden indicado. Bosch solo admite redes construidas según las reglas siguientes.

1. Para la conexión de centrales a la red, es necesario usar ETH1 y ETH2. Solo se debe usar un conmutador RSTP externo en ETH1 o ETH2 para la conexión de centrales en red.
2. Para conectar un OPC, FSM-5000-FSI, Praesideo/PAVIRO, UGM-2040, es necesario usar ETH3. Es posible conectar un conmutador RSTP externo, que no se debe utilizar para la conexión de centrales en red.
3. Para Remote Services, es necesario usar ETH4. Si no es necesaria ninguna conexión con Remote Services, es posible usar ETH4 para conectar un OPC, FSM-5000-FSI, Praesideo/PAVIRO o UGM-2040.
4. Si no hay conexión de la central a la red mediante ETH1 y ETH2, es posible usar cada una para conectar un OPC, FSM-5000-FSI, Praesideo/PAVIRO o UGM-2040.

5.1 Protocolos

SNMP

SNMP se usa para supervisar y controlar los componentes de red. Para ello, se pueden consultar o modificar los parámetros de los nodos de red. Necesitará un software de administración de redes adecuado (p. ej., HiVision de Hirschmann) para realizar esta tarea.

Aviso!

La red utiliza la cadena de comunidad SNMP fija:PUBLIC

Tenga en cuenta que la serie AVENAR panel todavía no es compatible con el protocolo SNMP.

LLDP

LLDP es un protocolo básico que sigue el estándar IEEE y que se usa para compartir información de red entre dispositivos próximos. La información se

– incluye en los datos SNMP y
– se muestra mediante el controlador de la central como parte de los datos del diagnóstico de red.

Protocolo RSTP

RSTP es un protocolo de red que sigue el estándar IEEE. RSTP garantiza que no existan lazos en las redes. Las rutas redundantes se detectan en la red, se desactivan y se activan cuando sea necesario (en caso de fallo de una conexión).
El protocolo se emplea exactamente para este fin en la red.
Los cambios que se realicen en la topología después de un fallo en la conexión se cancelan automáticamente una vez que se ha solucionado el error.

5.2 Diámetro de red

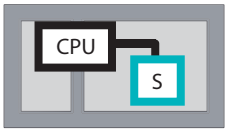
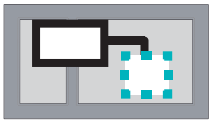
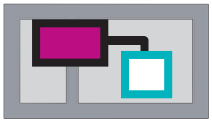
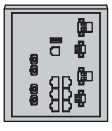
El diámetro de red de las redes de centrales Ethernet RSTP no debe ser mayor de 32.

Definición

El diámetro de una red equivale al número de conmutadores RSTP existentes en la sección más larga posible sin lazos entre 2 extremos en la red.
Tenga en cuenta lo siguiente respecto a una red de centrales Ethernet RSTP:

- Cada controlador de la central contiene un extremo y un conmutador RSTP interno.
- La combinación del controlador de la central y el controlador de la central redundante cuenta como un solo conmutador RSTP.
- Los conversores de medios no se consideran conmutadores RSTP.
- Las conexiones CAN no se incluyen en la sección más larga posible.
- Los servidores OPC no se tienen en cuenta al evaluar el diámetro.

Llave

	Procesador central en el controlador de la central o en teclado remoto.
	Conmutador interno RSTP en el controlador de la central o en el teclado remoto.
	Controlador de la central o teclado remoto con procesador central y conmutador interno RSTP.
	Controlador de la central redundante con procesador central y conmutador RSTP interno.
	Controlador de la central o teclado remoto Punto de inicio o punto final para calcular el diámetro de red en los ejemplos.
	Switch Ethernet como conmutador RSTP externo (en general, switch Ethernet MM)

El lazo más pequeño posible consta de 2 centrales conectadas. El diámetro de esta red equivale a 2, ya que los conmutadores RSTP internos están ubicados entre los extremos.

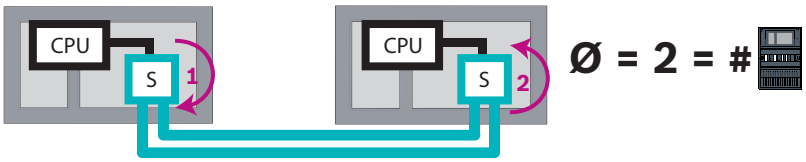


Figura 5.1: Diámetro de red de un lazo con dos centrales

En un lazo de centrales sin conmutadores RSTP externos, el diámetro de la red equivale al número de centrales instaladas.

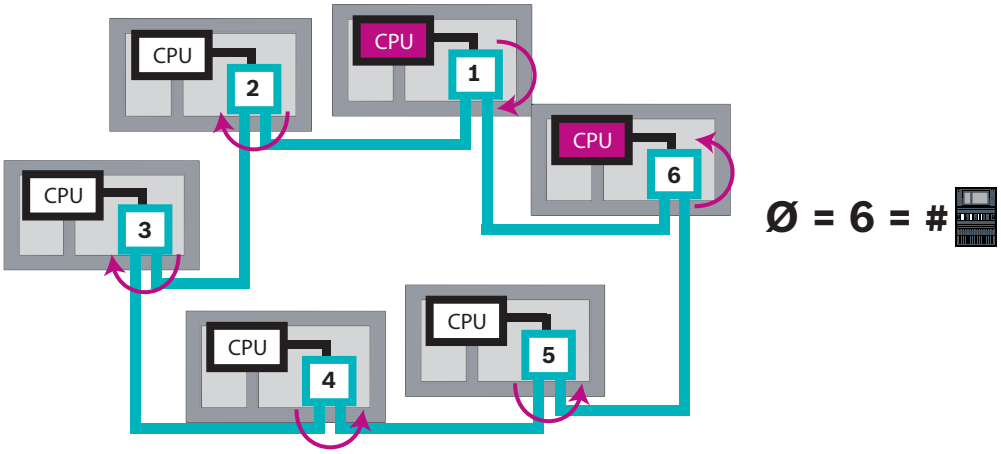


Figura 5.2: Diámetro de red de un lazo con 6 centrales

Si una red troncal y los sublazos conectados entre sí a través de los switch Ethernet, estos conmutadores RSTP externos también se deben tener en cuenta.

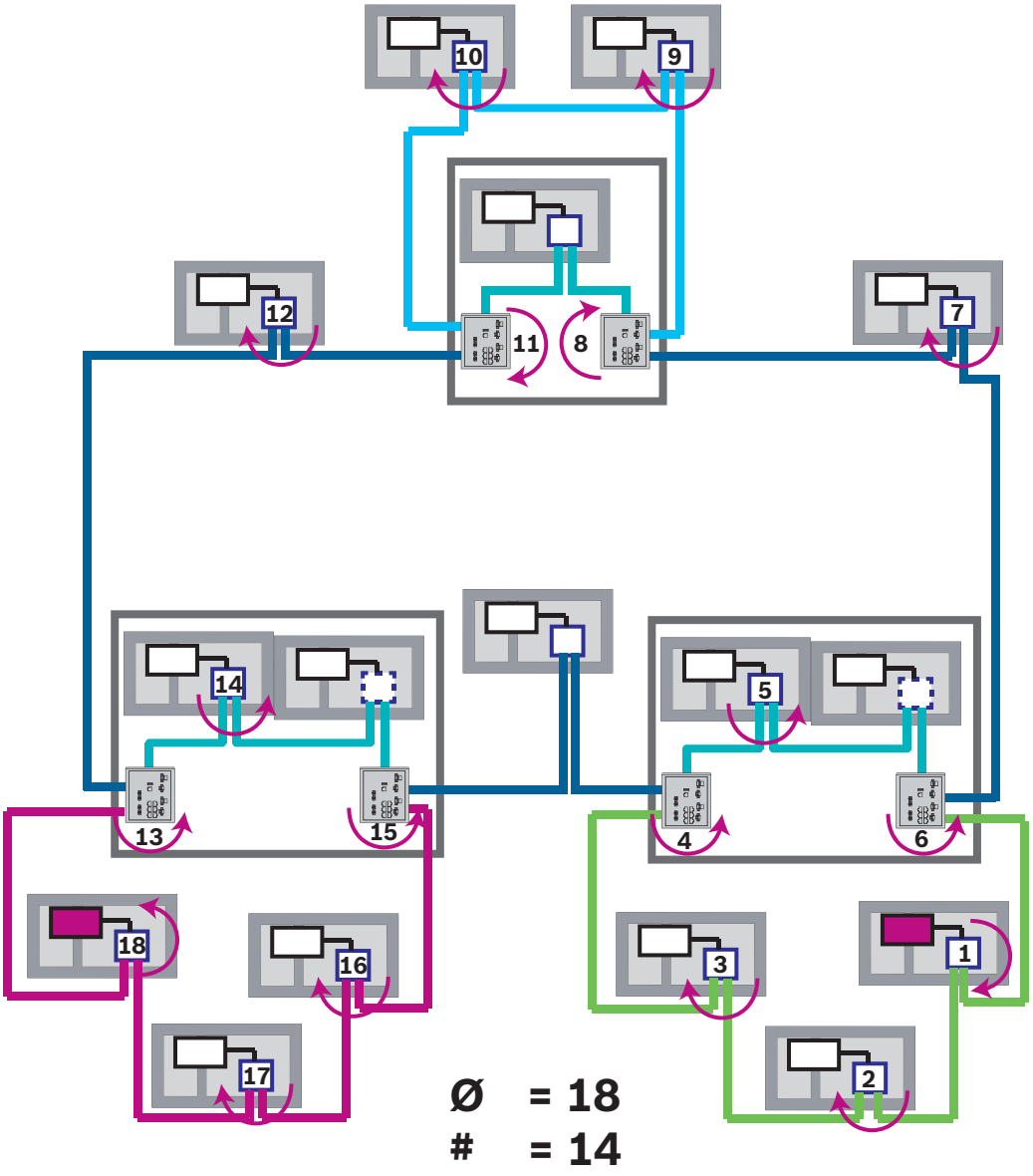


Figura 5.3: Diámetro de una red troncal con lazos secundarios

La figura muestra el diámetro que tiene para encontrar la ruta más larga.

5.3 Cables usados

Utilice solo los siguientes cables para el funcionamiento en red. El uso de otros cables no cumple los estándares de seguridad de las directivas de la CE.

– Cable Ethernet
  Cable de conexión Ethernet, apantallado, CAT 5e o superior.
  Tenga en cuenta el radio mínimo de curvatura indicado en las especificaciones del cable.
– Cable de fibra óptica
  Multimodo: cable de conexión Ethernet de fibra óptica, I-VH2G 50/125µ dúplex o I-VH2G 62.5/125µ dúplex, conector SC.
  Monomodo: cable de conexión Ethernet de fibra óptica, I-VH2E 9/125µ dúplex, conector SC.
  Tenga en cuenta el radio mínimo de curvatura indicado en las especificaciones del cable.

Aviso!
Longitud del cable TX
Todas las conexiones IP deben ser directas o a través de conversores de medios aprobados por Bosch. La longitud de cable TX entre nodos debe ser inferior a 100 m.

Aviso!
VdS 2540
Para cumplir los requisitos de VdS 2540 para las rutas de transmisión de datos utilice cable de fibra óptica para las conexiones Ethernet. Para las conexiones dentro de una carcasa, es posible usar cables Ethernet TX.

5.4 Creación o modificación de una red Ethernet

Hay varias formas de crear una red Ethernet de paneles de control de alarma de incendios. Los 2 procedimientos que se explican a continuación se diferencian en el tamaño de las redes y en el número de tareas de instalación y de configuración que se llevan a cabo en cada uno de ellos.

Reglas para usar 4 puertos Ethernet

Si la central tiene 4 puertos Ethernet, aplique las reglas siguientes en el orden indicado. Bosch solo admite redes construidas según las reglas siguientes.

1. Para la conexión de centrales a la red, es necesario usar ETH1 y ETH2. Solo se debe usar un conmutador RSTP externo en ETH1 o ETH2 para la conexión de centrales en red.
2. Para conectar un OPC, FSM-5000-FSI, Praesideo/PAVIRO, UGM-2040, es necesario usar ETH3. Es posible conectar un conmutador RSTP externo, que no se debe utilizar para la conexión de centrales en red.
3. Para Remote Services, es necesario usar ETH4. Si no es necesaria ninguna conexión con Remote Services, es posible usar ETH4 para conectar un OPC, FSM-5000-FSI, Praesideo/PAVIRO o UGM-2040.
4. Si no hay conexión de la central a la red mediante ETH1 y ETH2, es posible usar cada una para conectar un OPC, FSM-5000-FSI, Praesideo/PAVIRO o UGM-2040.

Crear una red Ethernet (proyectos pequeños)

Este procedimiento está pensado para proyectos que solo necesitan un pequeño número de ingenieros al mismo tiempo para instalar el sistema de detección de incendios.

1. Diseñe la red.
2. Cree la red en FSP-5000-RPS y configure los ajustes de red.
3. Imprima la información de la red y guárdela en un lugar seguro o en el portátil.
4. Instale las centrales y los cables de red y conecte estos componentes a una red.
5. Configure los ajustes de red de las centrales individuales directamente en la unidad de control, tal como se muestra en el documento impreso.
6. Reinicie los paneles de control en la red para activar la configuración de la red.
7. Conecte su ordenador con el software de programación FSP-5000-RPS instalado a un panel de control de la red. Cargue esta configuración en el resto de paneles de control de la red a través de este panel de control. Las centrales redundantes utilizan la configuración de la central principal.
8. Lleve a cabo una operación de reinicio (reset) para restablecer los mensajes de error pendientes. Corrija los errores que existan.

Configure primero los ajustes de red de las centrales, pues esto le ofrece la ventaja de poder programar los demás panels de control de la red desde un solo panel de control.

Crear una red Ethernet (proyectos medianos y grandes)

Este procedimiento está pensado para los proyectos en los que varios equipos deben realizar diversas tareas de forma simultánea. Debido a que en muchas de las tareas que se realizan durante la instalación y configuración es necesario reiniciar la central de alarma de incendios, la red no se inicia en este procedimiento hasta una fase posterior.

1. Diseñe la red.
2. Cree una configuración de la red sin periféricos con FSP-5000-RPS.
3. Imprima la información de la red y guárdela en un lugar seguro o en el portátil.
4. Instale los cables de red y compruebe las secciones o lazos.
5. Instale las centrales y póngalas en marcha como centrales independientes.
6. Instale los periféricos en las centrales.
7. Configure las centrales con FSP-5000-RPS.
8. Compruebe que las centrales individuales funcionan correctamente.
9. Ponga en marcha los lazos de la red de uno en uno, según la topología.
   Comience por la red troncal.
   - Cree una configuración para la red troncal en FSP-5000-RPS. Importe las configuraciones necesarias de la central. Configure los ajustes de red e imprímalos.
   - Conecte todas las centrales a una red.
   - Configure los ajustes de red de las centrales individuales directamente en el controlador de la central, tal como se muestra en el documento impreso.
   - Reinicie las centrales para cargar la configuración de la red.
   - Haga "ping" en las centrales próximas para comprobar la red.
   - Ponga en marcha la red troncal en su totalidad y corrija los errores que existan.

   Ponga en marcha los sublazos utilizando el mismo método que para la red troncal.

Agregar una central a una red

1. Cambie la configuración de red en FSP-5000-RPS.
2. Imprima la información de la red y guárdela en un lugar seguro o en el portátil.
3. Instale el panel de control y los cables de red y conecte estos componentes a la red.
4. Configure los ajustes de red del panel de control individual directamente en la unidad de control, tal como se muestra en el documento impreso.
5. Restablezca la central y las centrales adyacentes para activar la configuración de la red.

Quitar una central de la red

1. Cambie la configuración de red en FSP-5000-RPS.
2. Imprima la información de la red y guárdela en un lugar seguro o en el portátil.
3. Configure los ajustes de red de los paneles de control adyacentes directamente en la unidad de control, tal como se muestra en el documento impreso.
4. Desconecte la central y la fuente de alimentación (alimentación y batería) antes de quitarla de la red.
5. Restablezca las centrales adyacentes para activar la configuración de la red.

6 Red CAN

Topología de lazo

En una topología de lazo, el cable CAN siempre se enruta desde un terminal CAN1 a un terminal CAN2 [CAN1 ⇒ CAN2]. La longitud de cable depende de la sección transversal del cable.

Conexión CAN

La conexión CAN es una conexión de dos hilos (CAN-H y CAN-L). Conecte CAN-H a CAN-H y conecte CAN-L a CAN-L para establecer una conexión con dos hilos. En casos excepcionales, puede se necesaria una conexión de tres hilos (CAN-H, CAN-L y CAN-GND), por ejemplo con

una carga de EMC alta o una diferencia considerable en la tensión de derivación a tierra. Conecte CAN-H a CAN-H, CAN-L a CAN-L y CAN-GND a CAN-GND para establecer una conexión con tres hilos. La pantalla del cable de CAN solo se conecta a la carcasa de metal de la central en un lateral.

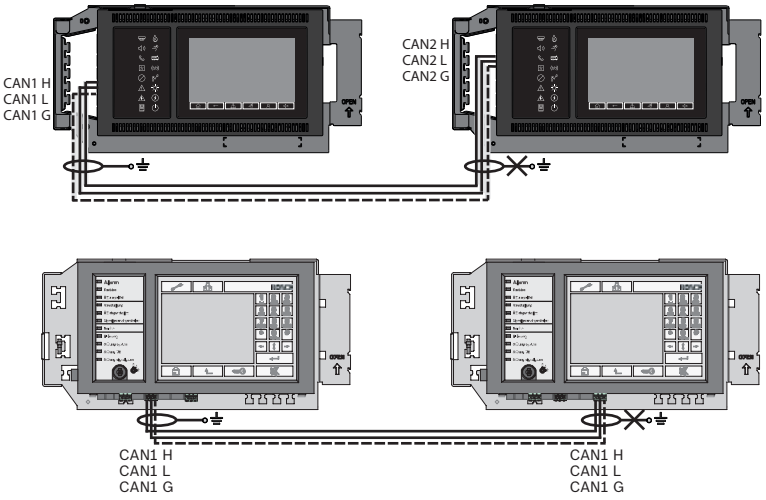


Figura 6.1: Conexión a CAN (superior: AVENAR, inferior: FPA)

Longitud de cable para funcionamiento en red

La longitud máxima de cable permitida depende de la resistencia del lazo del cable usado y del número de nodos de comunicación.

Ejemplo: cable del detector de incendios J-Y (St) Y 2 x 2 x 0,8 mm rojo permite conectar dos nodos a una distancia máxima de unos 800 m.

Aviso!

La distancia entre los dos nodos de una topología de lazo puede determinarse mediante la lectura del valor en dos nodos del diagrama.

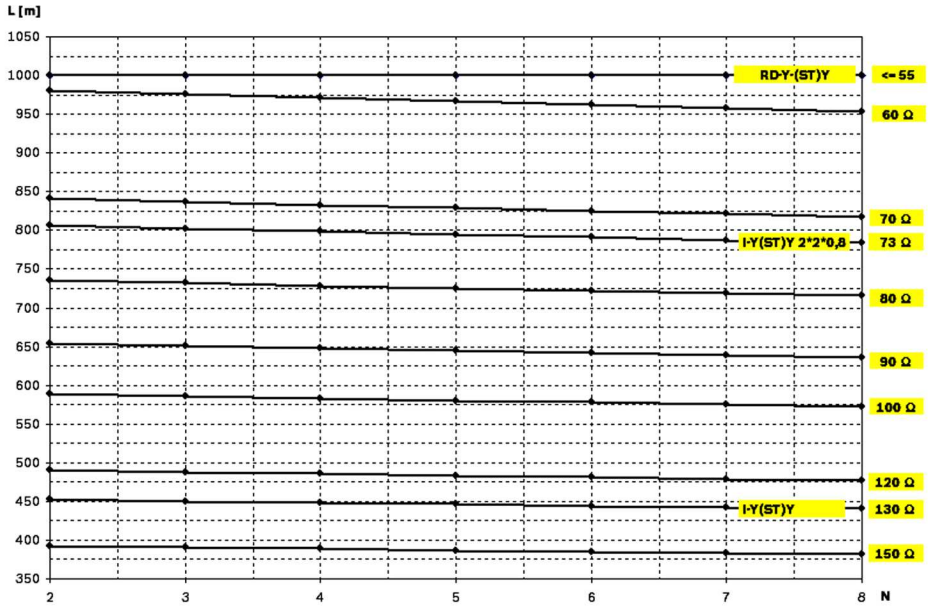


Figura 6.2: Red CAN: longitud de cable que se puede conseguir en función del número de nodos y de la resistencia del cable

L = longitud de cable en metros

N = número de nodos

6.1 Crear o modificar una red CAN

Este procedimiento está pensado para proyectos que solo necesitan un pequeño número de ingenieros al mismo tiempo para instalar el sistema de detección de incendios.

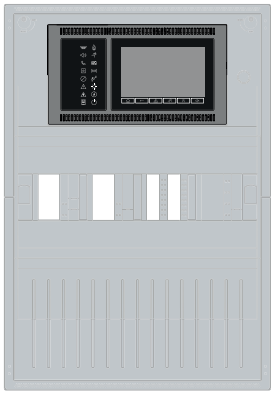
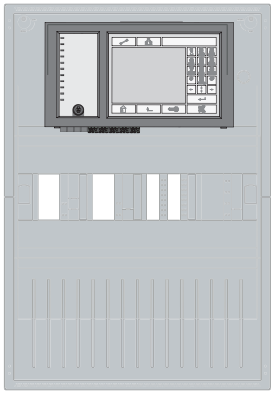
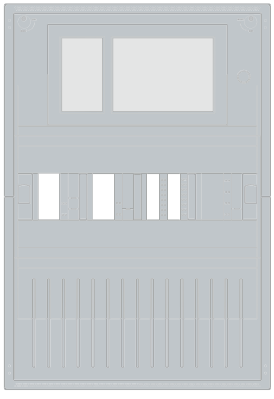
Procedimiento para crear una red CAN

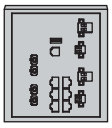
1. Diseñe la red.
2. Cree la red en FSP-5000-RPS.
3. Imprima la información de la red y guárdela en un lugar seguro o en el portátil.
4. Instale las centrales y conéctelas a una red mediante el uso de cables CAN.
5. Conecte su ordenador con el software de programación FSP-5000-RPS instalado a un panel de control de la red. Cargue esta configuración en el resto de paneles de control de la red a través de este panel de control. Las centrales redundantes utilizan la configuración de la central principal.
6. Lleve a cabo una operación de reinicio (reset) para restablecer los mensajes de error pendientes. Corrija los errores que existan.

7 Patrón de red Ethernet y CAN

Para crear redes de centrales correspondientes a las topologías presentadas y a los servicios de conexión, es necesario el patrón de funcionamiento en red descrito en este documento.

Icono	Descripción
	Cable Ethernet TX (cobre), longitud de cable TX entre nodos <100 m
	Cable Ethernet FX (cable de fibra óptica)

Icono	Descripción
	Cable Ethernet TX o FX, longitud de cable TX entre nodos <100 m
	Cable CAN
	Carcasa Nota: para simplificar la descripción de los distintos patrones de red, las figuras de este capítulo muestran siempre una pequeña carcasa de central para simbolizar una central. Sin embargo, esta pequeña carcasa **no** dispone de suficiente espacio para montar los conmutadores, los conversores de medios y las puertas de enlace que se necesitan en todos los casos que se presentan. Utilice el Safety Systems Designer para asegurarse de que solicita la cantidad correcta de carcasas y del tamaño correcto para instalar los equipos.
	AVENAR panel
	FPA
	AVENAR panel o FPA

Icono	Descripción
	Conmutador Ethernet como conmutador RSTP externo (en general, conmutador Ethernet MM)
	Conversor de medios
	Puerta de acceso a red segura para Remote Services
	Conexión a un servidor OPC, FSM-5000-FSI, Praesideo/PAVIRO o UGM-2040

7.1 Red de centrales sobre Ethernet

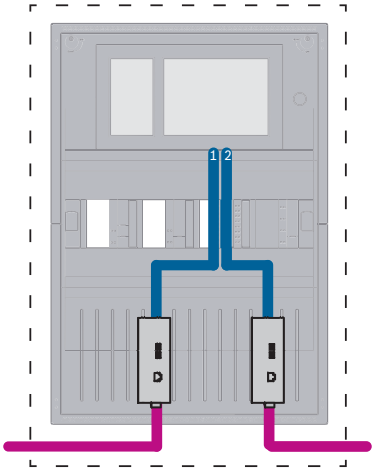


Figura 7.1: Red de centrales sobre Ethernet

Para rangos superiores a 100 m es obligatoria la extensión del alcance con conversores de medios. Para rangos inferiores a 100 m, puede que no sean necesarios los conversores de medios.

7.2 Red de centrales sobre CAN

Figura 7.2: Red de centrales sobre CAN

7.3 Servicios de conexión a la central

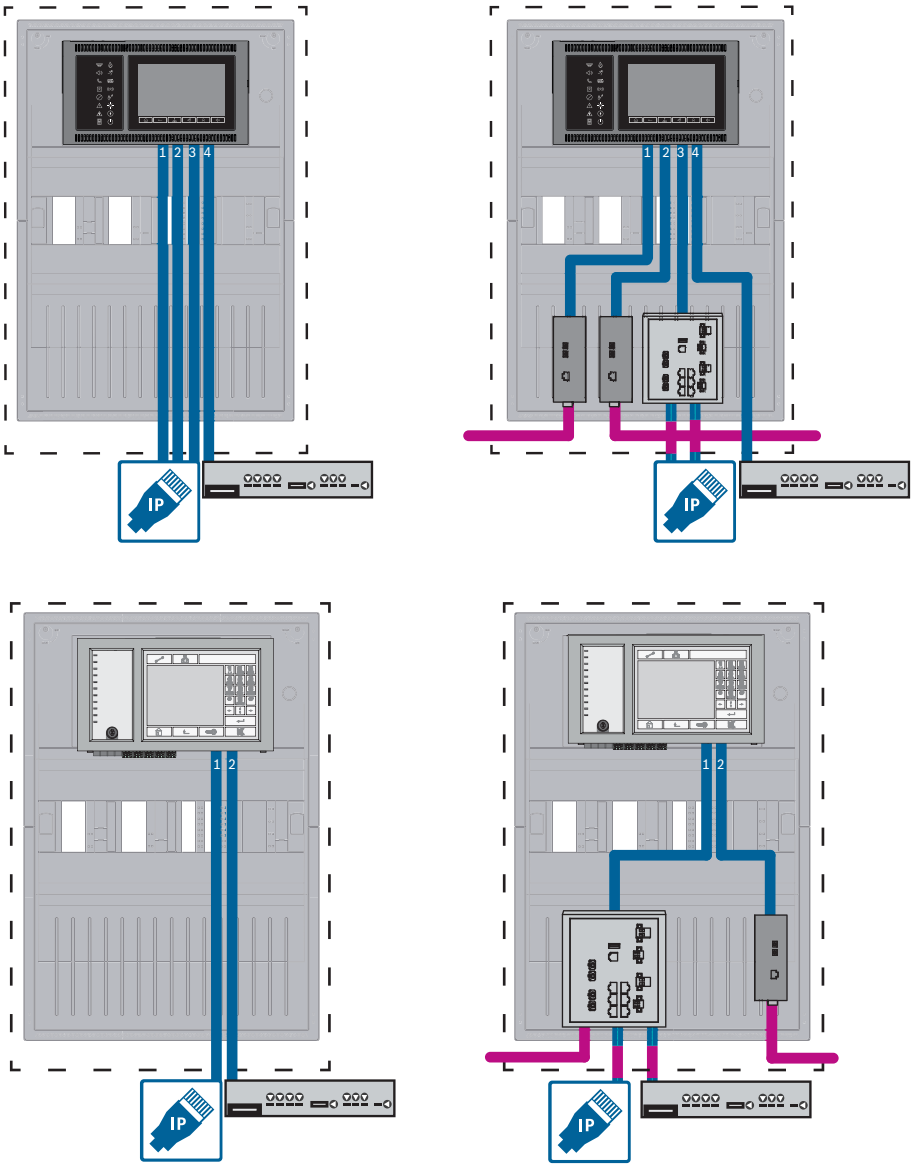


Figura 7.3: Lado izquierdo: sin red de centrales, lado derecho: con la red de centrales

Para rangos superiores a 100 m es obligatoria la extensión del alcance con conversores de medios. Para rangos inferiores a 100 m, puede que no sean necesarios los conversores de medios.

7.4 Red de centrales sobre Ethernet con centrales redundantes

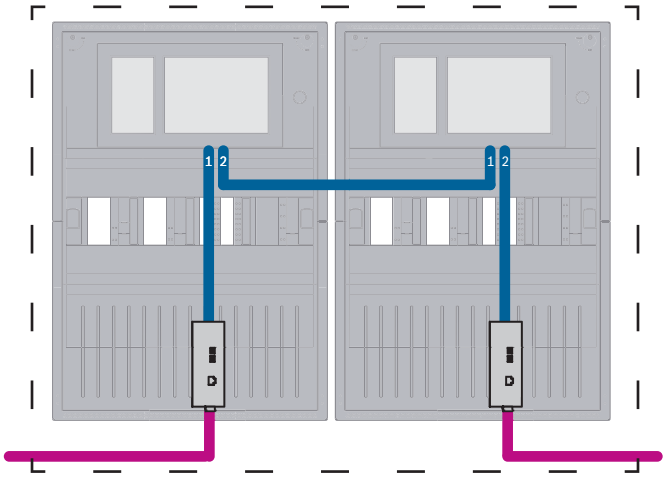


Figura 7.4: Red de centrales sobre Ethernet con centrales redundantes

Para rangos superiores a 100 m es obligatoria la extensión del alcance con conversores de medios. Para rangos inferiores a 100 m, puede que no sean necesarios los conversores de medios.

7.5 Red de centrales sobre CAN con centrales redundantes

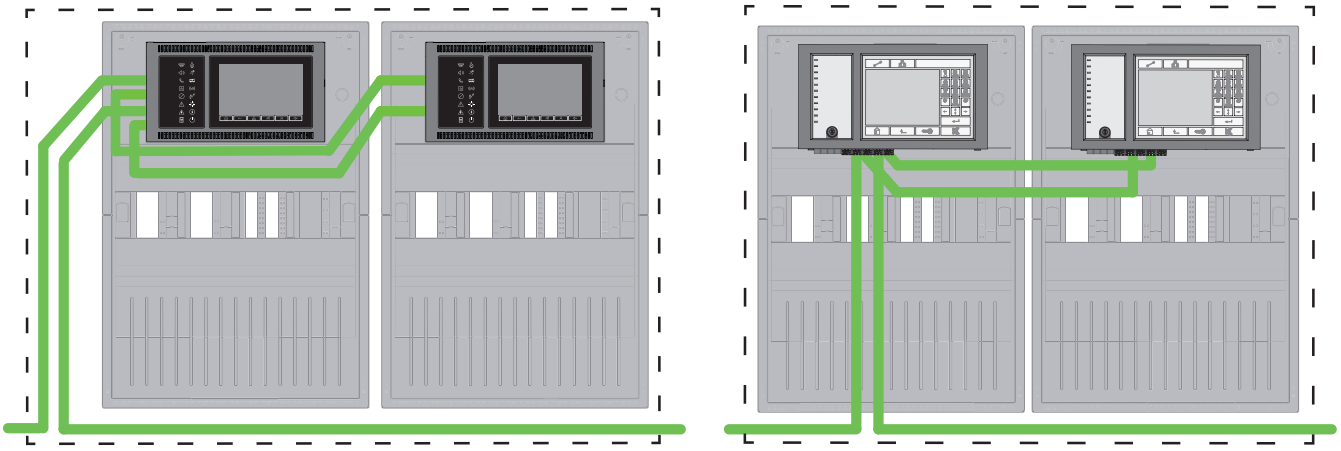


Figura 7.5: Red de centrales sobre CAN con centrales redundantes

7.6 Red de centrales sobre dos lazos Ethernet

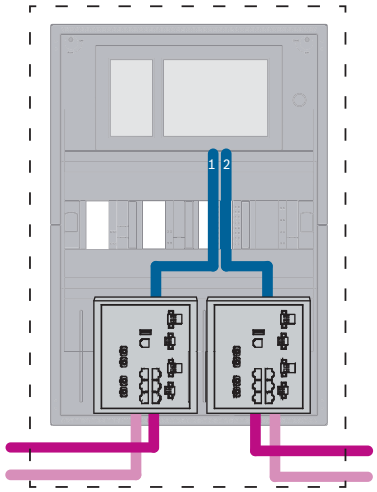


Figura 7.6: Conectar redes Ethernet

7.7 Red de centrales sobre dos lazos Ethernet con centrales redundantes

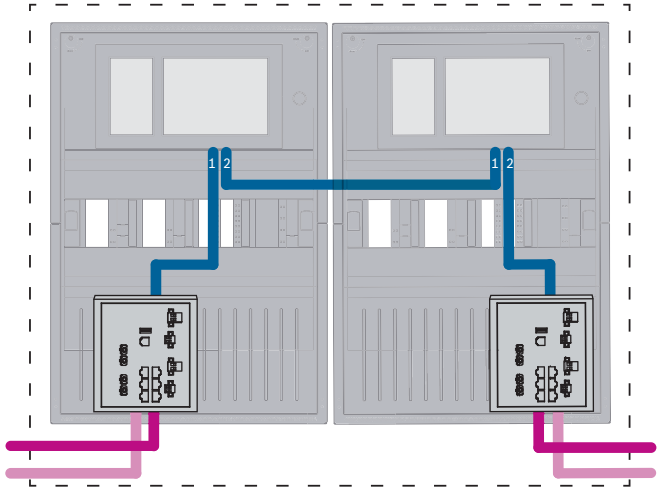


Figura 7.7: Conectar redes Ethernet con centrales redundantes

7.8 Conectar redes Ethernet y CAN con centrales redundantes

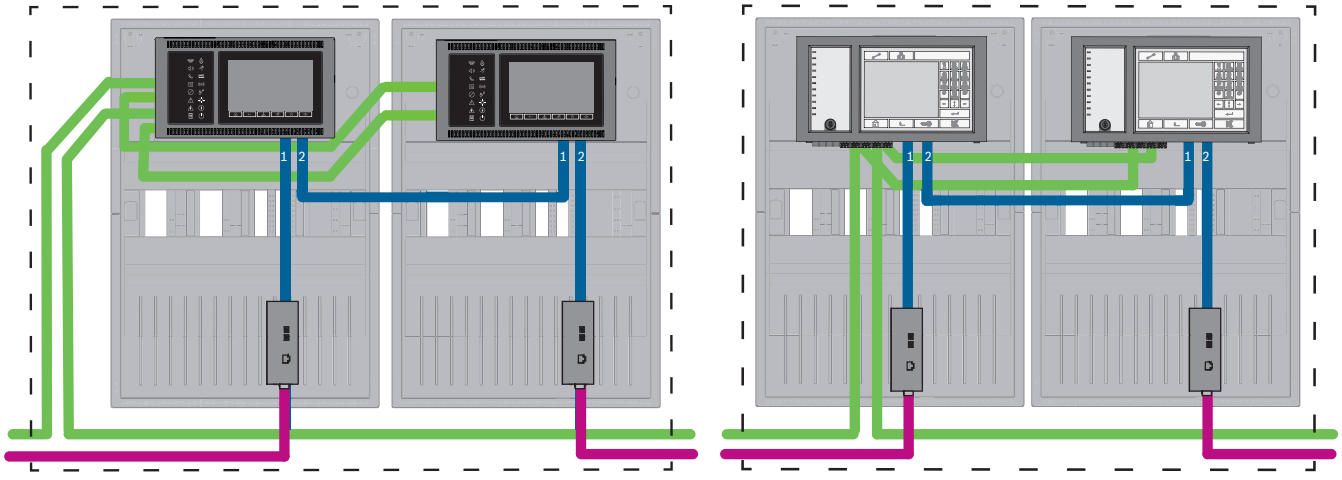


Figura 7.8: Conectar redes Ethernet y CAN con centrales redundantes

Para rangos superiores a 100 m es obligatoria la extensión del alcance con conversores de medios. Para rangos inferiores a 100 m, puede que no sean necesarios los conversores de medios.

7.9 Conectar servicios remotos a centrales redundantes

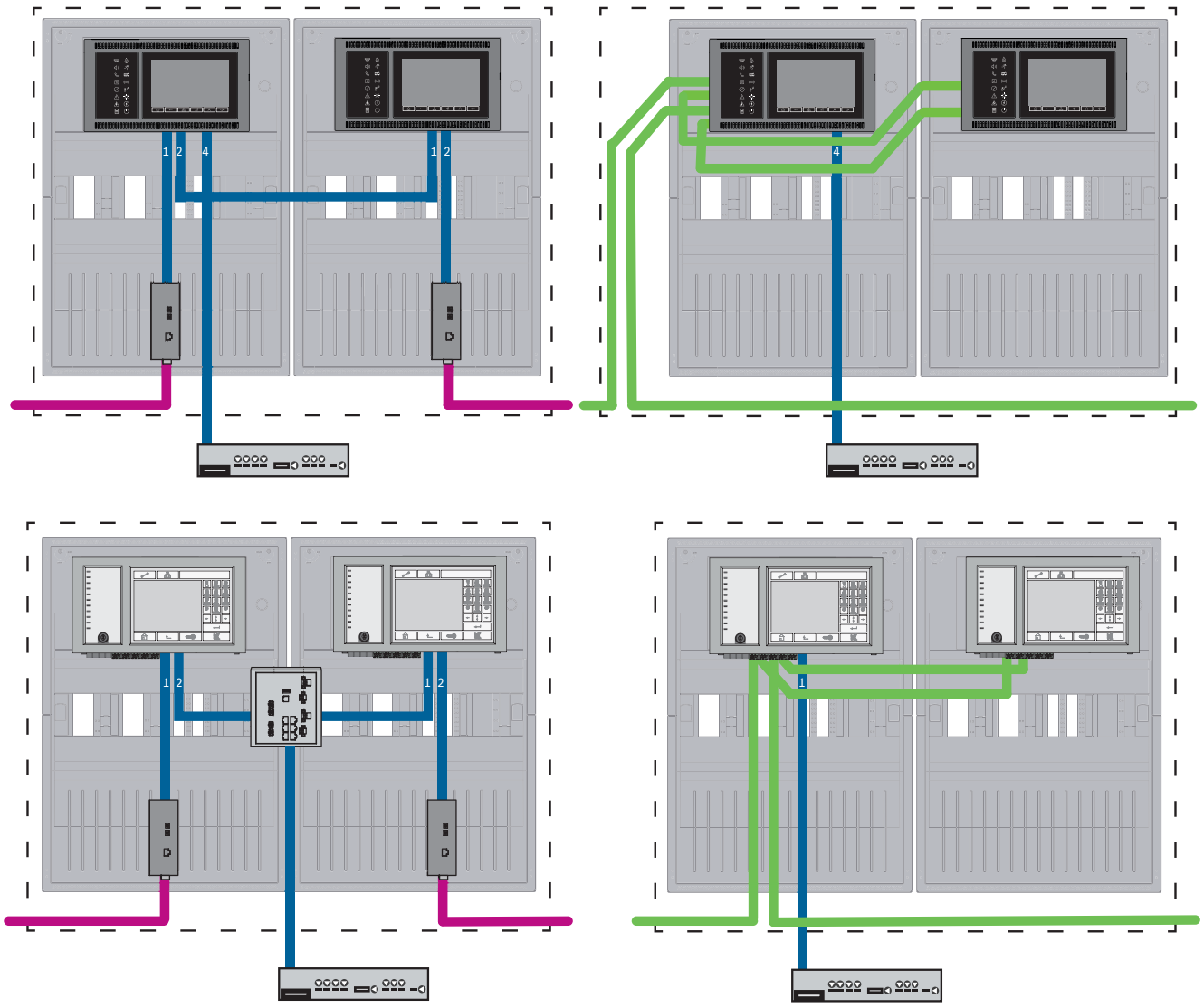


Figura 7.9: Lado izquierdo: en red Ethernet Lado derecho: en red CAN

Para rangos superiores a 100 m es obligatoria la extensión del alcance con conversores de medios. Para rangos inferiores a 100 m, puede que no sean necesarios los conversores de medios.

8 Remote Services

Los siguientes servicios pertenecen a Remote Services:

- Remote Connect
- Remote Alert
- Remote Maintenance

El requisito previo para Remote Alert y Remote Maintenance es Remote Connect.

8.1 Remote Connect

Remote Connect ofrece una conexión a Internet de confianza y segura, que permite el acceso remoto a una central a través de FSP-5000-RPS. Remote Connect es la base para todos los Remote Services. Para Remote Connect utilice la puerta de acceso a red segura.
Si se trata de una red de centrales, una de las centrales de dicha red tiene que estar conectada a una puerta de acceso a red segura. Esta es la única conexión que tiene que ser una conexión Ethernet dedicada.

Aviso!
Mientras que Remote Connect admite la conexión a una red de centrales a través de Ethernet o CAN, las funciones Remote Alert y Remote Maintenance solo se admiten cuando existe una conexión Ethernet entre las centrales y esta se configura para el uso en el servicio.

La función Remote Connect debe estar habilitada en la configuración de FSP-5000-RPS de esta central.
En la siguiente topología se muestran controladores de central conectados por Ethernet donde una puerta de acceso a red segura está conectada a la red mediante un switch Ethernet (normalmente MM).

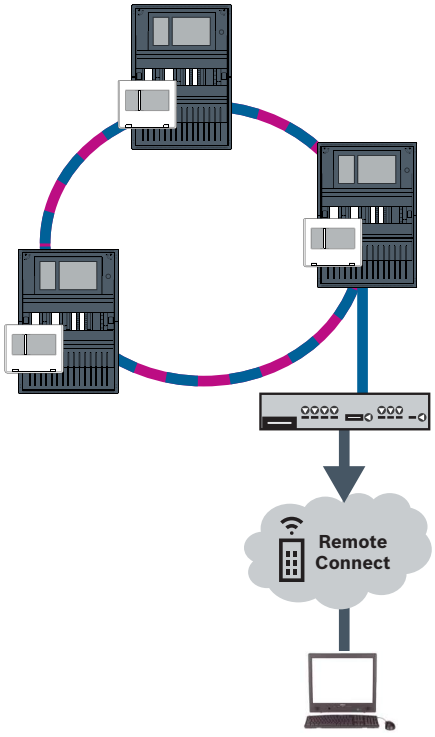


Figura 8.1: Remote Connect en un lazo Ethernet

Aviso!
Para conectar los paneles a través de FX, utilice los conversores de medios mediante Bosch.

Para evitar el envío de tráfico multidifusión (multicast) relevante EN 54-2 al router, utilice el switch Ethernet (normalmente MM, BPA-ESWEX-RSR20) certificado con la versión 2.8 de la central. Active el snooping IGMP del switch Ethernet, consulte la sección correspondiente en el capítulo de Instalación de la Guía de funcionamiento en red.

Aviso!
El router de Internet (o la red de la empresa que proporciona acceso a Internet), así como la puerta de acceso a red segura, deben proporcionar subredes separadas. Las centrales de la red de centrales no se puede colocar en la subred del router de Internet. La superposición de redes secundarias tampoco es posible.
Cuando las subredes se superponen, es necesario separarlas cambiando las direcciones IP en la parte de la red dedicada a la central.
Además, tiene que propagar los cambios de la puerta de acceso a red segura Para ello, abra la interfaz de la web mediante un navegador web:
- Dirección: https://192.168.1.254
- Nombre de usuario: bosch
- Contraseña: ipti83

En **Configuración** -> **Red (LAN)** puede cambiar la dirección IP. Tenga en cuenta que la dirección de **Puerta acc pred:** especificada en la configuración del controlador de la central debe coincidir con la dirección IP de la puerta de acceso a red segura.

Aviso!
De acuerdo con las directrices de DIBt, no se permite el restablecimiento remoto a través de Remote Services para restablecer el estado operativo de sistemas de control de puertas con ayuda de apertura motorizada.

En la siguiente topología se muestra una red CAN donde se ha conectado una puerta de acceso a red segura a la red a través de un puerto Ethernet.

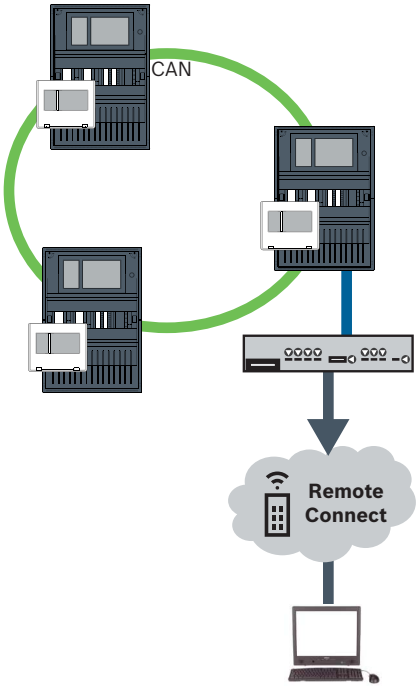


Figura 8.2: Remote Connect en un lazo CAN

8.2 Remote Alert

A través de Remote Alert, una central muestra la información de estado correspondiente a Remote Portal.
Los datos transferidos se analizan con Remote Alert. En caso de un evento inesperado, se notifica al usuario vía SMS y/o correo electrónico acerca de las alertas recibidas.
Remote Alert también está disponible para Private Secure Network.

8.3 Remote Maintenance

Remote Maintenance ofrece la posibilidad de supervisar de forma remota ciertos parámetros de diversos elementos de seguridad conectados a una central de incendio. Remote Portal permite ejecutar varios modos de prueba.

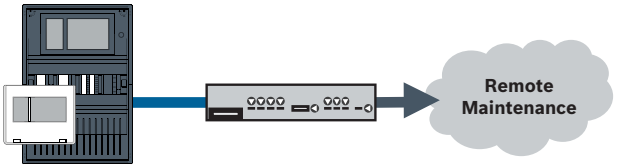


Figura 8.3: Remote Maintenance

Aviso!
Las conexiones Ethernet que se usan solo para transferir datos de Remote Maintenance se pueden realizar con cables Ethernet o cables de fibra óptica. Tenga en cuenta la longitud máxima permitida para los cables.

Aviso!
Para conectar los paneles a través de FX, utilice los conversores de medios mediante Bosch.

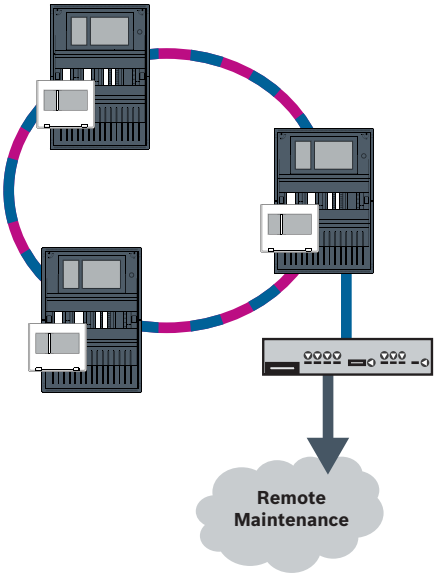


Figura 8.4: Remote Maintenance

Al usar Remote Maintenance en redes Ethernet, se debe conectar una central de la red al router para transferir datos. Todos los datos recopilados se transfieren desde la red a través de esta conexión.

Remote Maintenance para Remote Portal

Remote Maintenance recopila datos de dispositivos y módulos funcionales LSN importantes y los envía a Remote Portal, donde se analizan y visualizan para actividades de mantenimiento.

Remote Maintenance para una red segura privada

Remote Maintenance puede configurarse para Private Secure Network; en este caso, los datos recopilados se envían al sistema de servidor de gestión central (CMS).

Precaución!

Los Remote Services requieren una conexión IP segura. Se requiere BoschRemote Services o conexión con Private Secure Network.
Con Private Secure Network se proporciona una red IP basada en DSL con un acceso inalámbrico opcional en el lado de la central (EffiLink). Remote Services para Private Secure Network solo está disponible en Alemania con un acuerdo de servicios con Bosch BT-IE.

Aviso!

Para conectar los paneles a través de FX, utilice los conversores de medios mediante Bosch.

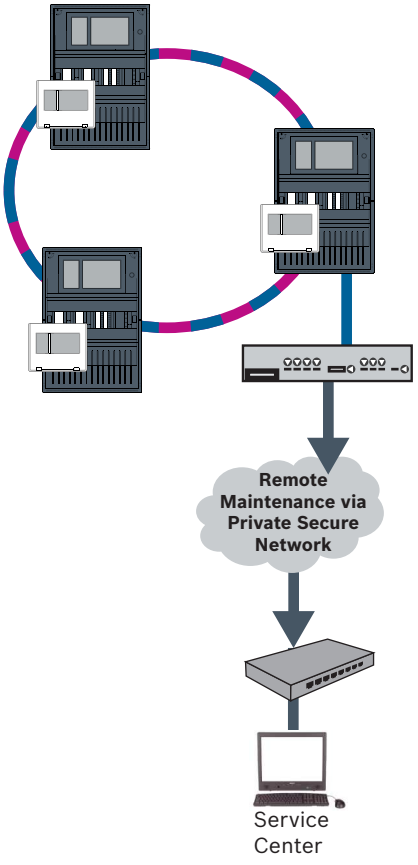


Figura 8.5: Remote Maintenance para una red segura privada

Para Remote Maintenance, es necesario introducir la dirección IP IP del servidor y el puerto del servidor del sistema Remote Maintenance en el software de programación FSP-5000-RPS. Asigne un ID de red de central único a la red.

El conmutador que se usa para conectar el CMS se debe programar por separado.
Programe la dirección IP y los ajustes de redundancia del conmutador, consulte *Ajustes del conmutador, Página 45*. Como el conmutador se instala en las inmediaciones directas (sin espacio intermedio), no es necesario diseñar la fuente de alimentación de manera redundante y, por tanto, las salidas de avería no se usan.
Asegúrese de que los ajustes RSTP de los controladores de la central, en FSP-5000-RPS y en el switch Ethernet son idénticos.

8.4 Remote Portal

Requisitos

Aviso!
Para evitar tener que volver a realizar configuraciones o ajustes cuando utilice Remote Services, asegúrese de que se cumplen los siguientes requisitos:
- la central tiene instalado el firmware 2.19.7 o superior, todas las centrales están conectadas a través de Ethernet, los módulos Ethernet están habilitados y se han configurado los ajustes Ethernet estándar;
- Remote Connect se ha habilitado en la configuración de la central FSP-5000-RPS;
- Puerta de acceso a red segura para Remote Services disponible
- el ordenador tiene FSP-5000-RPS 4.8 o superior instalado y dispone de acceso a Internet.

Aviso!
Evite la actualización de la puerta de acceso a red segura durante la conexión.
Las actualizaciones de la puerta de acceso a red segura se ejecutan periódicamente en las primeras horas de la mañana. Por lo tanto, especifique la zona horaria en **System** -> **General Settings** -> **Timezone**.

Instrucciones
Para poder utilizar Remote Services, debe ser usuario de una cuenta de Remote Portal

Paso 1: Crear una cuenta Remote Portal
Puede haber varios usuarios en una cuenta Remote Portal. Cada cuenta Remote Portal tiene un único Remote ID, que está diseñado para representar una empresa. Si no se puede utilizar una cuenta Remote Portal existente, tiene que crear una:

1. En https://remote.boschsecurity.com -> **Sign Up** introduzca su nombre, su empresa y dirección de correo electrónico, y cree una contraseña. Consulte las condiciones de uso y seleccione **I agree to the terms and conditions** (Acepto las condiciones de uso). Tenga en cuenta también la declaración de privacidad y seleccione **I agree to the privacy statement** (He leído y acepto la política de privacidad).
2. Haga clic en **Registrarse**.
   Remote Portal le enviará de inmediato un mensaje por correo electrónico a la dirección indicada con un enlace para la activación.
3. Para activar la cuenta, haga clic en el enlace de activación. En Remote Portal haga clic en su nombre de usuario y seleccione **Account Settings**. Aquí encontrará su Remote ID. Necesitará más adelante este Remote ID en el controlador de la central.

Para que cada uno de sus técnicos disponga de su propia cuenta, puede crear varios usuarios con el mismo Remote ID:
Iniciará sesión en Remote Portal.

- Seleccione **Users** -> **New Technician**. Después introduzca los datos solicitados y confirme haciendo clic en **Save**.

Paso 2: Conectar puerta de acceso a red segura
Para establecer Remote Services utilice una puerta de acceso a red segura.

1. Conecte el puerto WAN de la puerta de acceso a red segura al router de Internet o a la red de la empresa que proporcione acceso a Internet.
2. En el router de Internet o en la red de empresa compruebe la disponibilidad de los siguientes protocolos y puertos para la puerta de acceso a red segura (es necesario para la conexión a Remote Services).

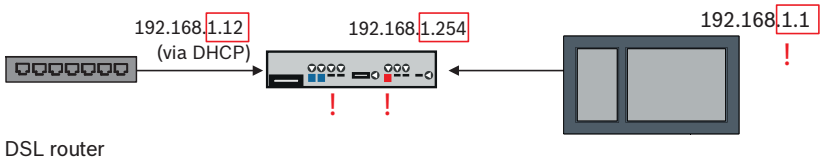
Protocolo	Puerto predeterminado	Descripción
HTTP	80 y 8080	para registro de Remote Connect yRemote Maintenance
IPsec VPN	UDP 500 y UDP 4500	para Remote Connect

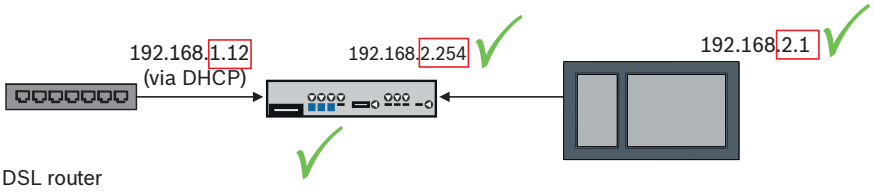
3. Conecte el puerto LAN1 de la puerta de acceso a red segura al puerto Ethernet del controlador de la central que utilice el cable de red CAT5 RJ45 suministrado. Observe las posibles topologías.
4. Conecte la puerta de acceso a red segura a un suministro de alimentación de 100 V - 230 V que utilice la alimentación suministrada.

El LED WAN está encendido (color azul) cuando se ha establecido la conexión a Internet. El LED VPN que se enciende (color azul) poco después, indica que se ha establecido una conexión VPN con Remote Portal.
Cada central o red de centrales conectada tiene un System ID único.

Separación de subredes (LED VPN apagado)

La conexión de la puerta de acceso a red segura para Remote Services falla en caso de que se solapen las subredes (LED VPN apagado). El ejemplo siguiente muestra una puerta de acceso de red segura y un controlador de central en el mismo rango de direcciones que el router DSL.





Una puerta de acceso a red segura detecta el solapamiento de subredes inequívocamente: el LED Alarm parpadea de forma continuada.
Para separar las subredes, es necesario cambiar el tercer octeto de la dirección IP. Cambie la dirección IP en el lado de la red de centrales. Después de cambiar la dirección IP , es necesario propagar los cambios a la puerta de acceso a red segura. Para ello, abra la interfaz de la web mediante un navegador web:
- Dirección: https://192.168.1.254
- Nombre de usuario: bosch
- Contraseña: ipti83

En **Configuración** -> **Red (LAN)** puede cambiar la dirección IP. Tenga en cuenta que la dirección de **Puerta acc pred:** especificada en la configuración del controlador de la central debe coincidir con la dirección IP de la puerta de acceso a red segura.

Paso 3: Establecer una conexión remota

1. Utilice los ajustes estándar de Ethernet en la central.
2. Reinicie la central.
3. Para la autenticación, seleccione **Configuration** -> **Network Services** -> **Change date / time**, introduzca la fecha actual y confirme los ajustes.
4. Seleccione **Configuration** -> **Network Services** -> **Remote Services** e introduzca el Remote ID.

Para comprobar el estado de la conexión remota: seleccione **Diagnóstico** -> **Servicios de red** -> **Servicios remotos** en el controlador de la central.

Paso 4: Asignar la licencia en Remote Portal

Para poder usar Remote Services, debe asignar una licencia en Remote Portal. La licencia se suministra de forma automática a la cuenta la primera vez que se establece la conexión correctamente.

Aviso!

No es posible volver a asignar ni suspender una licencia ya asignada.

1. En la página https://remote.boschsecurity.com, introduzca su dirección de correo electrónico y su contraseña y haga clic en **Login**.
2. Seleccione **Systems**.
3. Elija el sistema deseado.
4. En **Services**, haga clic en el botón **Add Service** que aparece debajo del servicio en cuestión.
5. La licencia se renovará automáticamente por defecto (**Service Settings**, opción **With Auto-Renew**).
6. Haga clic en **Save** para confirmar la configuración.

Una vez asignada la licencia puede usarse el servicio correspondiente. La licencia asignada se muestra con una marca de verificación verde.

Paso 5: volver a pedir licencia

1. Pedir licencias de un año del sistema de detección de incendios de Bosch. Cada red necesita sus propias licencias.
   Bosch envía un correo electrónico a la dirección proporcionada. El mensaje de correo electrónico incluye los números de registro de licencia correspondientes a la cantidad de licencias pedidas, así como instrucciones y un enlace a Remote Portal.
2. En la página https://remote.boschsecurity.com, introduzca su dirección de correo electrónico y su contraseña y haga clic en **Login**.
3. Seleccione **Licenses**.
4. Haga clic en el botón **+**.
5. Siga las instrucciones indicadas en la ventana **Add Licenses** y confirme haciendo clic en **Save**.
6. Se ha actualizado la lista de licencias.

9 Sistemas de alarma por voz

En la siguiente topología se muestran los controladores de la central conectados a través de Ethernet, donde el sistema Praesideo/PAVIRO se integra en el lazo de centrales mediante un módulo de interfaz Ethernet.

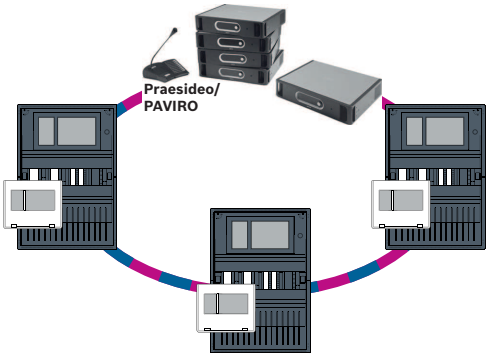


Figura 9.1: Lazo Ethernet con Praesideo/PAVIRO

Utilice Ethernet Switch (normalmente MM BPA-ESWEX-RSR20) certificado con la versión 2.8 de firmware de la central.
Para evitar el envío de tráfico de multidifusión relevante de EN 54-2 al sistema Praesideo/PAVIRO, active el snooping IGMP snooping del MM; consulte la sección correspondiente en el capítulo de Instalación de la Guía de funcionamiento en red.
En cada controlador de la central de una red CAN se puede conectar un sistema Praesideo/PAVIRO utilizando un módulo de interfaz Ethernet. En la siguiente topología se muestran controladores de central conectados a través de CAN, donde el sistema Praesideo/PAVIRO se conecta a un controlador de central mediante un módulo de interfaz Ethernet.

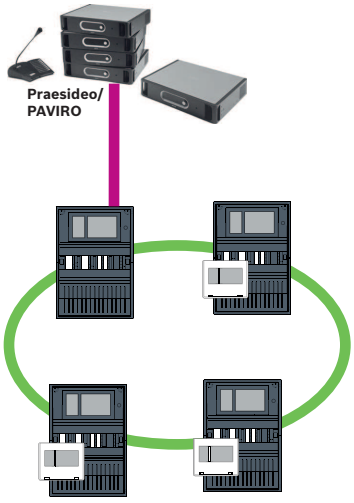


Figura 9.2: Praesideo/PAVIRO: conexión a una red CAN

Aviso!
Como el tráfico de la red CAN no se transfiere a través de la conexión Ethernet, debe desactivar el funcionamiento en red por IP en el software de programación de FSP-5000-RPS. Si no se desactiva, la red no cumplirá los requisitos de la normativa EN 54.

Aviso!
Si un panel de control MPC-xxxx-B se va a usar para la conexión directa con un sistema Praesideo/PAVIRO, se necesita un cable de conexión cruzado, ya que ni Praesideo/PAVIRO ni MPC-xxxx-B admiten MDI(X) automático.

10 Instalación

Lista de comprobación

Antes de empezar con la instalación de la red, revise todos los puntos que se exponen a continuación.

- Ethernet y CAN
  - Las longitudes de línea requeridas de los cables Ethernet TX, Ethernet FX, CAN TX y CAN FX son inferiores a su longitud máxima.
  - También se programa todo el diseño de periféricos y su cableado en cada central.
- Diseño de la red
  - Se diseñan los ajustes de red y las direcciones IP de las centrales individuales, así como los componentes de red adicionales, y se ponen a su disposición.
  - Se le ofrece una descripción general de los componentes adicionales que se van a instalar, como switch Ethernet y conversores de medios, además del cableado de conexión con las centrales próximas.

- Hay una descripción general de la topología de red que se va a instalar disponible para su consulta.
- Se diseñan todos los ajustes de redundancia de red y se ponen a disposición para su consulta.

10.1 Ajustes del conversor de medios

Solo es necesario realizar unos pasos para usar el conversor de medio:
- Configure los interruptores DIP.
- Conecte el conversor de medio a los cables de red FX y CAT5e.
- Suministre alimentación al conversor de medio a través del módulo de controlador de baterías BCM interno.

Aviso!
Los conversores de medio solo se pueden alimentar a través del terminal de fuente de alimentación 1.
Por tanto, el LED de error del conversor de medio permanece encendido continuamente, aunque esto no afecta a la funcionalidad del dispositivo.

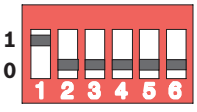
Aviso!
Utilice solo los siguientes cables para el funcionamiento en red:
Cable Ethernet
Cable de conexión Ethernet, apantallado, CAT5e o superior.
Tenga en cuenta el radio mínimo de curvatura indicado en las especificaciones del cable.
Cable de fibra óptica
Multi modo: cable de conexión Ethernet de fibra óptica, I-VH2G 50/125µ dúplex o I-VH2G 62.5/125µ dúplex, enchufe SC.
Modo sencillo: cable de conexión Ethernet de fibra óptica, I-VH2E 9/125µ dúplex
Tenga en cuenta el radio mínimo de curvatura indicado en las especificaciones del cable.

Aviso!
Consulte las guías de instalación de los kits de montaje para obtener información sobre cómo instalar un conversor de soportes en la de una central: FPM 5000 KMC(F.01U.266.845)FPM-5000-KES(F.01U.266.844)

Aviso!
La distancia de transmisión máxima para conversores de medio multimodo a través de FX es 2.000 m.
La distancia de transmisión máxima para conversores de medio de modo sencillo a través de FX es 40 km.

Configure el conversor de medio mediante los interruptores DIP, según se indica en la siguiente figura.

Aviso!
Cambie los ajustes del conmutador DIP en los conversores de medio únicamente cuando estén desactivados.



Número de interruptor DIP	Ajuste
1	Función "Link Fault Pass-Through" activada
2	Ethernet: modo automático
3	Ethernet: 100 MBit
4	Ethernet: dúplex completo
5	Cable de fibra óptica: dúplex completo
6	Enlace inactivo: desactivado

10.2 Instalación del switch Ethernet

Advertencia!
Luz láser
No mire directamente al haz de luz a simple vista ni a través de instrumentos visuales de ningún tipo (p. ej., una lupa o microscopio). El incumplimiento de este aviso supone un peligro para los ojos a una distancia inferior a 100 mm. La luz procede de los terminales visuales o del extremo de los cables de fibra óptica conectados a ellos. Diodo láser de CLASE 2M, longitud de onda 650 nm, salida <2 mW, de acuerdo con IEC 60825-1.

Aviso!
Consulte: Guía de instalación para el kit de montaje para switch Ethernet FPM-5000-KES (F.01U.260.523).

10.3 Ajustes del conmutador

Para utilizar los switches en la red, debe programarlos.
Conecte el portátil a la red y use el software HiDiscovery suministrado por el fabricante para llevar a cabo las tareas de programación iniciales de los switches. Con ayuda del software, busque los switches en la red. Haga doble clic en un switch para seleccionarlo y asignarle una dirección IP.
Después de la programación inicial de la dirección IP, use un explorador web para llamar al módulo de interfaz de usuario de configuración del switch.

Aviso!
Consulte la guía del usuario del fabricante para ver una descripción exacta de la instalación y configuración de los switches. Datos de acceso:
Usuario: admin
Contraseña: private

Utilice un explorador para llamar a la interfaz de usuario de configuración de los switches.
Configure los siguientes ajustes en el switch:
- *Asignación de una dirección IP, Página 46*,
- *Programación de los ajustes de redundancia, Página 46*.

Existen otros ajustes opcionales, p. ej.:
- *Programación del relé de avería, Página 47*,
- *Programación del control de conexión, Página 48*,
- *Activación de la operación snooping IGMP, Página 48*.

10.3.1 Asignación de una dirección IP

Aviso!
Consejo práctico:
En la parte del dispositivo donde están las direcciones IP, utilice números mayores que 200 (xxx.xxx.xxx.200) para los conmutadores, si la configuración de la red lo permite. Esto le permitirá una mejor separación del identificador de host de una dirección IP.
Ejemplo:
El conmutador 192.168.1.201 se asigna a la central con la dirección IP 192.168.1.1.

Aviso!
Consulte los siguientes documentos del fabricante para ver una descripción exacta de la instalación y configuración de los conmutadores:
Guía del usuario de instalación
Guía de referencia del módulo de interfaz basado en web

Utilice un explorador para ir al módulo de interfaz de usuario de configuración de los conmutadores.
En el menú **Basic Settings -> Network** (Ajustes básicos -> Red), establezca los siguientes valores en función de la topología seleccionada:
- Modo: local
- Dirección IP: la dirección IP requerida, p. ej., 192.168.1.201
- Máscara de red: la máscara de red requerida, p. ej., 255.255.255.0
- Puerta de acceso: la puerta de acceso requerida, p. ej., 192.168.1.254 o 0.0.0.0 si no se requiere ninguna puerta de acceso.

Haga clic en **Write** (Aceptar).

Aviso!
Los ajustes realizados en los elementos de menú de la configuración del conmutador se implementan después de hacer clic en **Write** (Aceptar).
Si desea guardar los ajustes únicamente de forma permanente para conservarlos incluso después de reiniciar el dispositivo, en **Basic Settings -> Load/Save** (Ajustes básicos -> Cargar/Guardar), en el campo **Save** (Guardar), seleccione la opción **On the device** (En el dispositivo) y haga clic en el botón **Save** (Guardar).

10.3.2 Programación de los ajustes de redundancia

Como las redes de la central FPA usan RSTP como protocolo de redundancia, debe activar y programar el protocolo en el módulo de interfaz de usuario de comunicación:
En el menú **Redundancy -> Spanning Tree -> Global** (Redundancia -> Árbol de expansión -> Global), establezca los siguientes valores:
- Función: On
- Versión de protocolo: RSTP
- Configuración de protocolo: use los mismos ajustes que para los controladores de la central.

Haga clic en **Write** (Aceptar).

Aviso!
Los ajustes realizados en los elementos de menú de la configuración del conmutador se implementan después de hacer clic en **Write** (Aceptar).
Si desea guardar los ajustes únicamente de forma permanente para conservarlos incluso después de reiniciar el dispositivo, en **Basic Settings -> Load/Save** (Ajustes básicos -> Cargar/Guardar), en el campo **Save** (Guardar), seleccione la opción **On the device** (En el dispositivo) y haga clic en el botón **Save** (Guardar).

10.3.3 Programación del relé de avería

Aviso!
El relé de avería solo se debe programar para las aplicaciones en las que se cumple al menos uno de los siguientes requisitos:
Existe una conexión entre dos switches. Esto ocurre en el caso de una red troncal con sublazos, por ejemplo.
La fuente de alimentación del switch se ha diseñado de manera redundante.

Aviso!
Consulte los siguientes documentos del fabricante para ver una descripción exacta de la instalación y configuración de los switches:
Guía del usuario de instalación
Guía de referencia del módulo de interfaz basado en web

Utilice un explorador para ir al módulo de interfaz de usuario de configuración de los switches.
En **Diagnosis -> Signal Contact** (Diagnóstico -> Contacto de señal), en la pestaña **Signal Contact 1** (Contacto de señal 1), establezca **Signal Contact Mode** (Modo de contacto de señal) en **Device Status** (Estado del dispositivo).
En **Diagnosis -> Device Status** (Diagnóstico -> Estado del dispositivo), en el campo **Monitoring** (Control), establezca los siguientes valores:
- **Alimentación 1**: **Monitor**
- **Error de conexión**: **Monitor**

Los demás ajustes se deben establecer en **Ignore** (Ignorar).

Aviso!
Los ajustes de **Device Status** (Estado del dispositivo) también se aplican al LED de avería del switch.

Haga clic en **Write** (Aceptar).

Aviso!
Los ajustes realizados en los elementos de menú de la configuración del switch se implementan después de hacer clic en **Write** (Aceptar).
Si desea guardar los ajustes únicamente de forma permanente para conservarlos incluso después de reiniciar el dispositivo, en **Basic Settings -> Load/Save** (Ajustes básicos -> Cargar/Guardar), en el campo **Save** (Guardar), seleccione la opción **On the device** (En el dispositivo) y haga clic en el botón **Save** (Guardar).

10.3.4 Programación del control de conexión

Aviso!
Solo es necesario configurar el control de conexión si va a usar el relé de avería del conmutador.

Si desea usar el relé de avería para controlar la conexiones del conmutador, especifique los puertos que se van a controlar en la configuración del conmutador.
Active la casilla **Forward Connection Error** (Reenviar error de conexión) de los puertos en el menú **Basic Settings -> Port Configuration** (Ajustes básicos -> Configuración de puertos).
Solo se controlan las conexiones para las que se ha activado la opción **Forward Connection Errors** (Reenviar errores de conexión).
Haga clic en **Write** (Aceptar).

Aviso!
Los ajustes realizados en los elementos de menú de la configuración del conmutador se implementan después de hacer clic en **Write** (Aceptar).
Si desea guardar los ajustes únicamente de forma permanente para conservarlos incluso después de reiniciar el dispositivo, en **Basic Settings -> Load/Save** (Ajustes básicos -> Cargar/Guardar), en el campo **Save** (Guardar), seleccione la opción **On the device** (En el dispositivo) y haga clic en el botón **Save** (Guardar).

10.3.5 Prioridad de QoS (solo para UGM-2040)

Si utiliza conmutadores para la comunicación entre redes FPA y el UGM-2040, se debe configurar la prioridad de QoS en los conmutadores del UGM.
En el menú QoS/Priorität -> Global (QoS/Prioridad -> Global), cambie los ajustes del campo de la lista desplegable de Trusted Mode a trustIpDscp.
Haga clic en **Write** (Aceptar).

Aviso!
Los ajustes realizados en los elementos de menú de la configuración del conmutador se implementan después de hacer clic en **Write** (Aceptar).
Si desea guardar los ajustes únicamente de forma permanente para conservarlos incluso después de reiniciar el dispositivo, en **Basic Settings -> Load/Save** (Ajustes básicos -> Cargar/Guardar), en el campo **Save** (Guardar), seleccione la opción **On the device** (En el dispositivo) y haga clic en el botón **Save** (Guardar).

10.3.6 Activación de la operación snooping IGMP

Para evitar el envío de tráfico de multidifusión relevante de EN 54-2 a otros sistemas conectados a Ethernet Switch (Praesideo/PAVIRO, Remote Connect) active la operación de snooping de IGMP.
En la página de configuración de IGMP del Ethernet Switch de , seleccione las siguientes opciones:

1. Active la operación snooping de **IGMP**.
2. Active el **IGMP Querier** (Generador de consultas IGMP).
3. Configure el intervalo de transmisión en el que el RSR20 envía paquetes de consulta IGMP (p. ej., 4 segundos).
4. Configure el tiempo en el que los miembros del grupo de multidifusión deben responder a las consultas de IGMP (p. ej., 3 segundos).
5. Seleccione **Discard** (Descartar) para los paquetes con direcciones de multidifusión desconocidas.

6. Seleccione **Send to Query and registered Ports** (Enviar a puertos registrados y de consulta) para los paquetes con direcciones de multidifusión conocidas.
7. Active IGMP solo para los puertos a los cuales estén conectados otros sistemas conectados al switch. Desactive la opción **Static Query Port** (Puerto de consulta estático) para todos los puertos.

10.4 Red CAN

Funcionamiento en red e interfaces

El controlador de la central tiene

– dos interfaces CAN (CAN1/CAN2) para el funcionamiento en red (topología de lazo o ramal).
– dos entradas de señal (IN1/IN2)
– dos módulos de interfaz Ethernet
– Interfaz USB

Según el tipo de controlador de central:

– dos interfaces Ethernet más
– Interfaz RS232

Tenga en cuenta que la longitud de cable máxima para conectar con el módulo de interfaz USB es de 3 m y para el módulo de interfaz RS232 es de 2 m.

Direccionamiento y ajustes en la red

Según el tipo de controlador de central:

– Dirección del nodo físico configurado en el firmware de la central al encender la central por primera vez
– RSN en los interruptores rotatorios mecánicos de la parte posterior de la central

Para mostrar la dirección del nodo físico, si está guardada en el controlador de la central:

▸ Seleccione **Configuración** -> **Servicios de red** -> **Ethernet** -> **Usar ajustes Ethernet** -> **Ajustes IP** -> **Ajustes predet**

Para cambiar la dirección del nodo físico, guardada en el controlador de la central:

▸ Muestre la configuración predeterminada y cambie el último número de la **dirección IP**.

Para cambiar un RSN mecánico:

▸ Establezca el RSN en los conmutadores giratorios mecánicos de la parte posterior de la central y anótelo en el símbolo debajo de los conmutadores giratorios.

Configuración de la topología

Los conmutadores DIP para la configuración de topologías diferentes se encuentran en la parte posterior.

▸ Marque el ajuste seleccionado en el símbolo cerca de los conmutadores DIP.

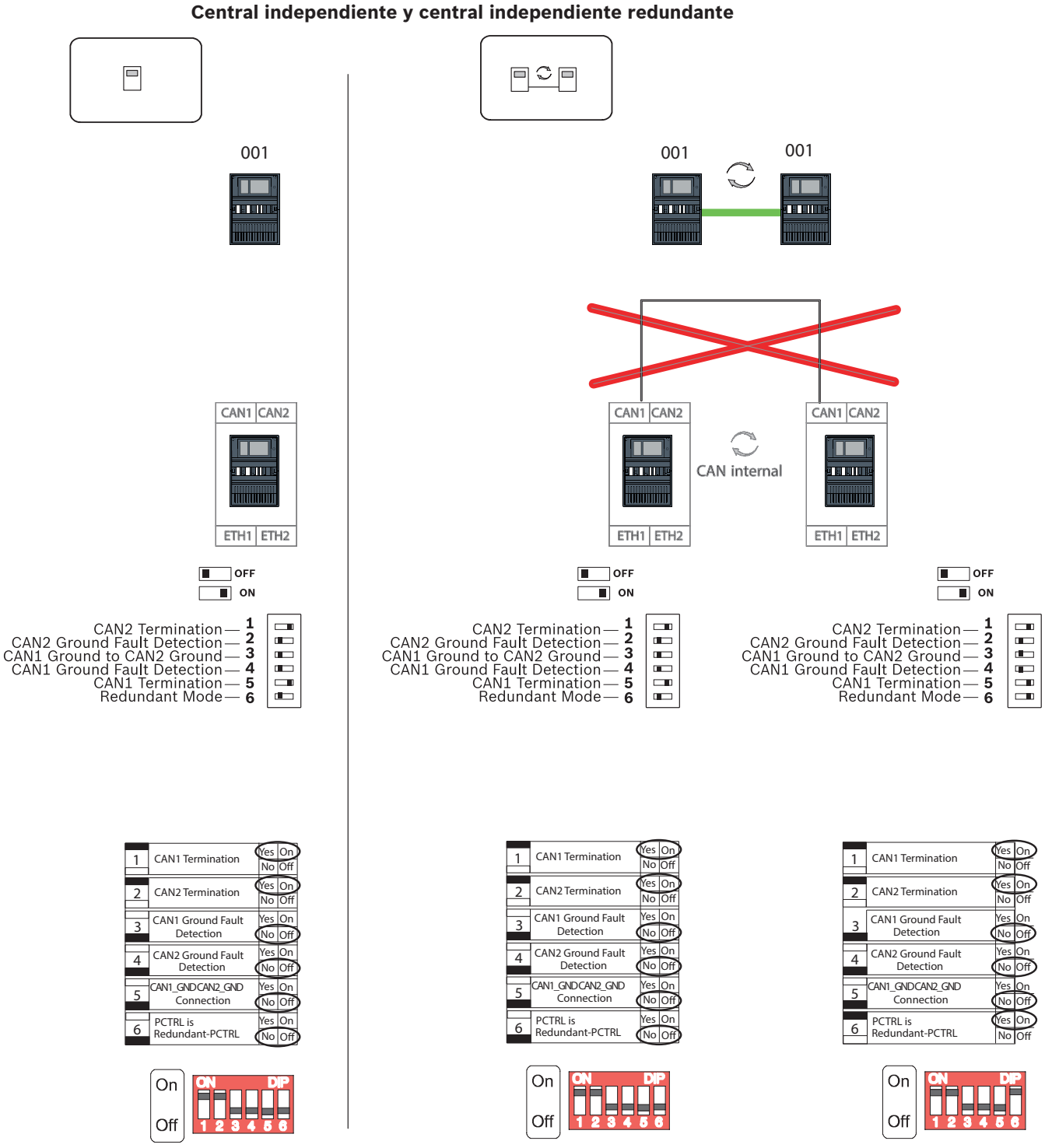


Figura 10.1: Ajustes de los conmutadores DIP para centrales autónomas (superior: AVENAR, inferior: FPA, izquierda: normal, derecha: redundante)

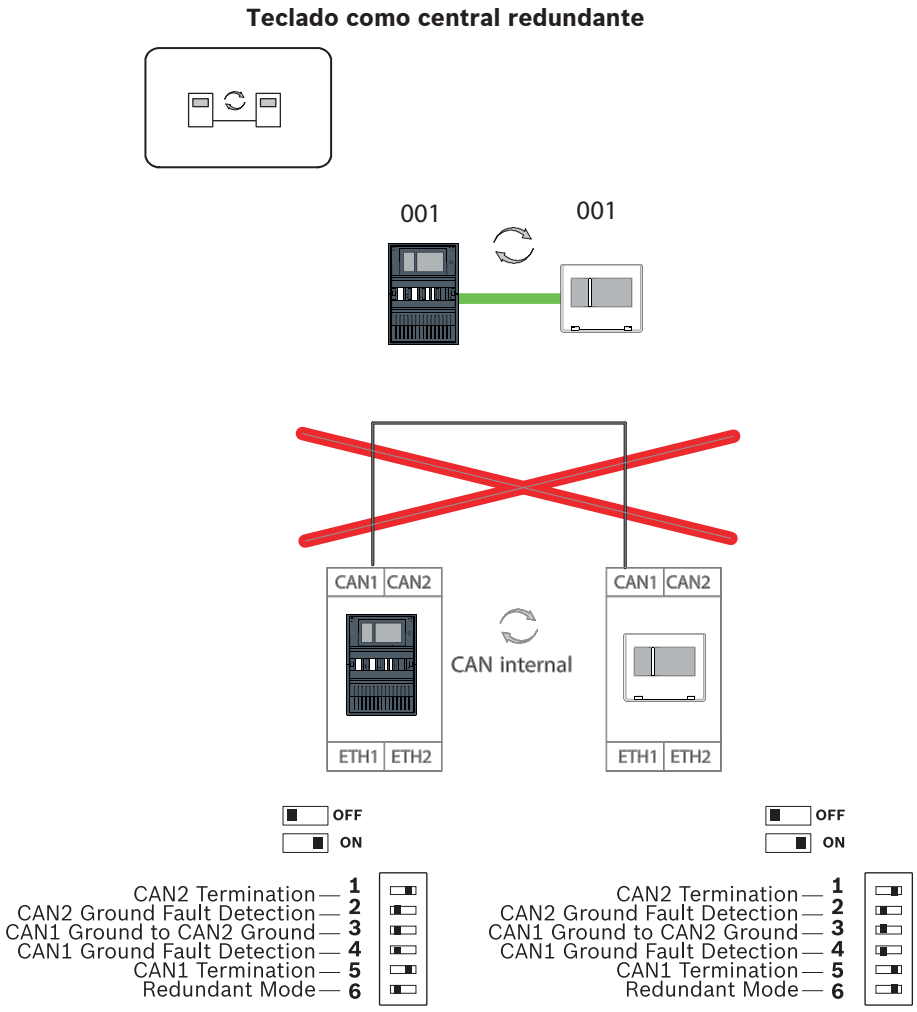


Figura 10.2: Ajustes de los conmutadores DIP para el teclado remoto como central redundante (solo AVENAR)

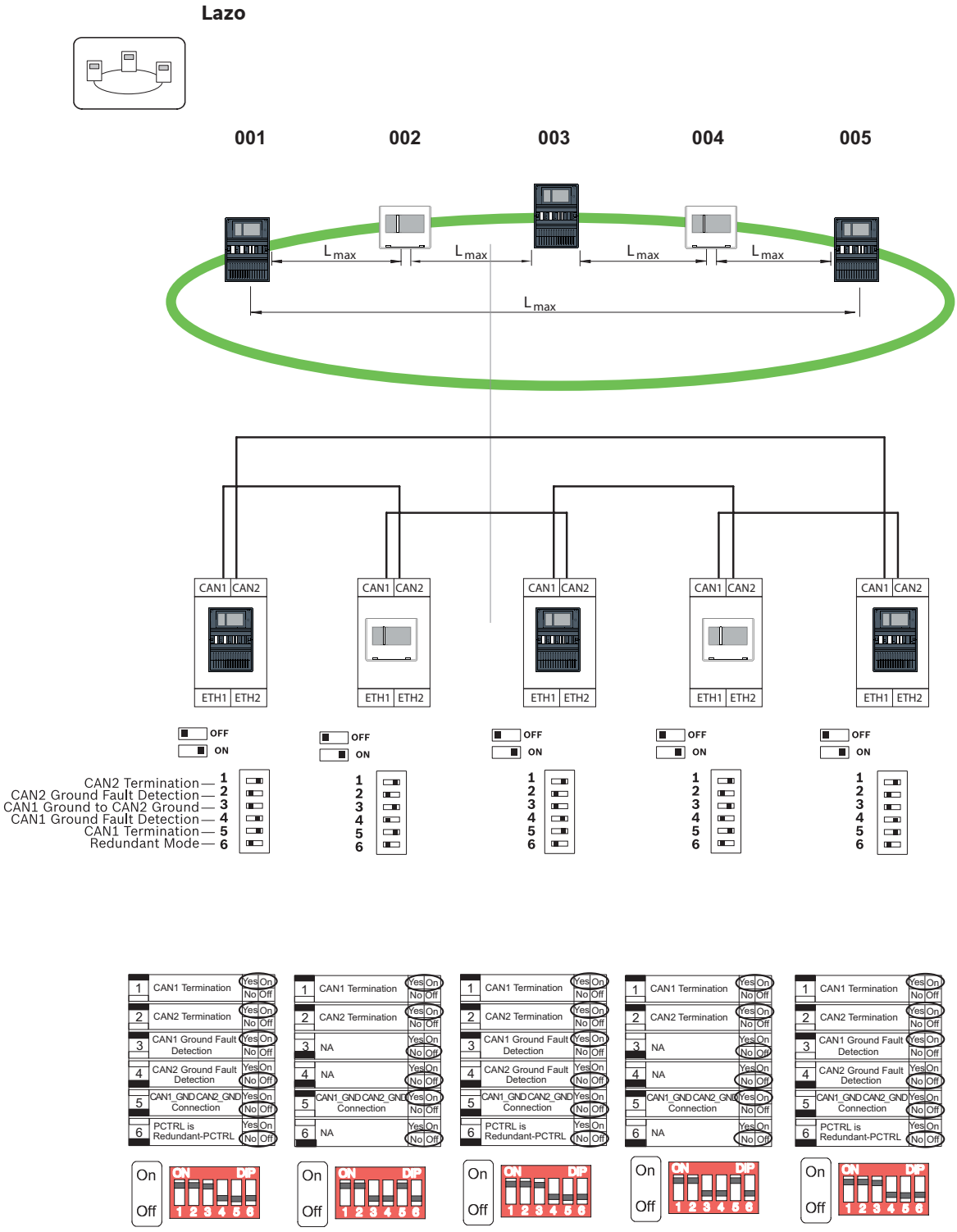


Figura 10.3: Ajustes de los conmutadores DIP para lazo (superior: AVENAR, inferior: FPA)

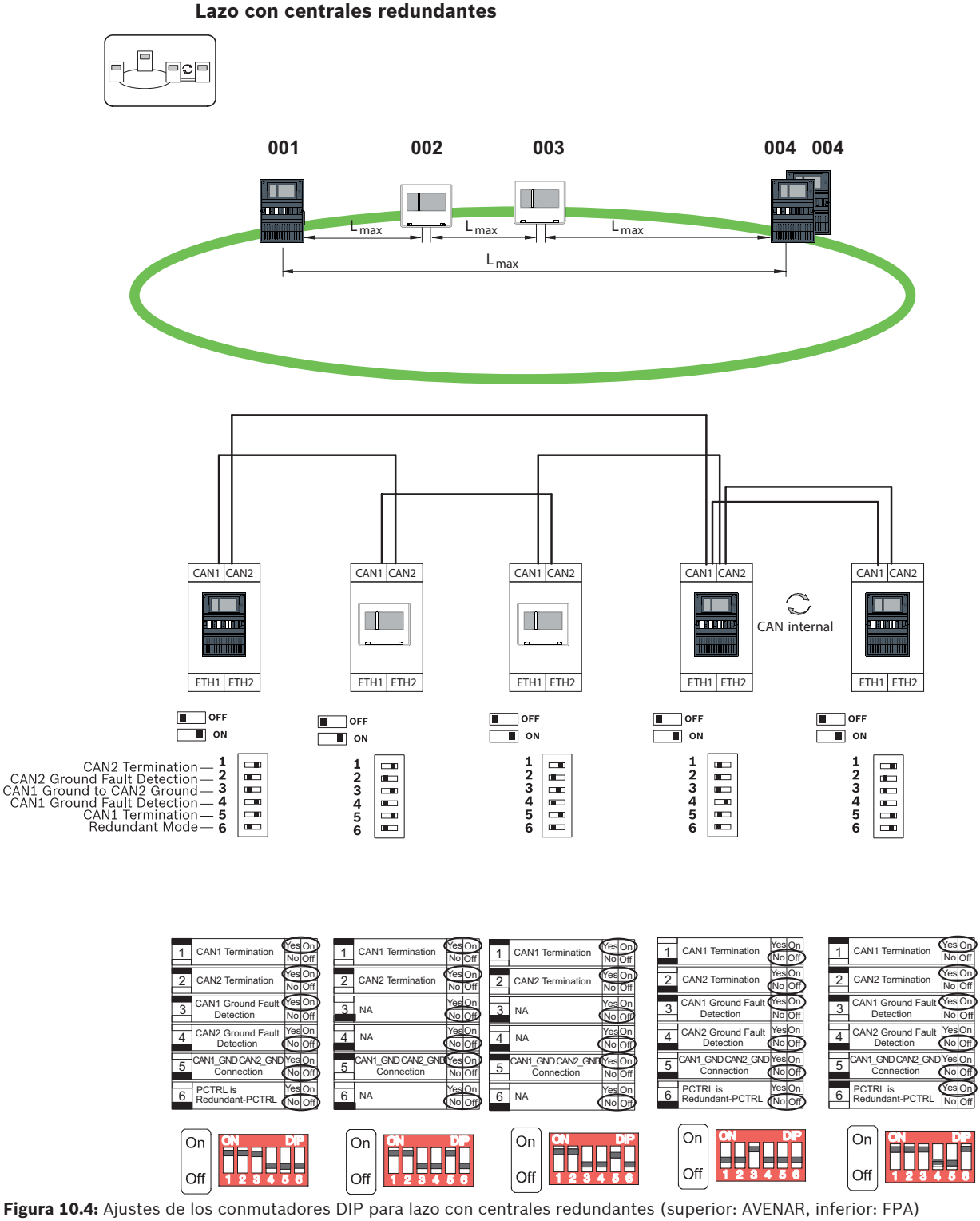


Figura 10.4: Ajustes de los conmutadores DIP para lazo con centrales redundantes (superior: AVENAR, inferior: FPA)

Lazo con teclado remoto como central redundante

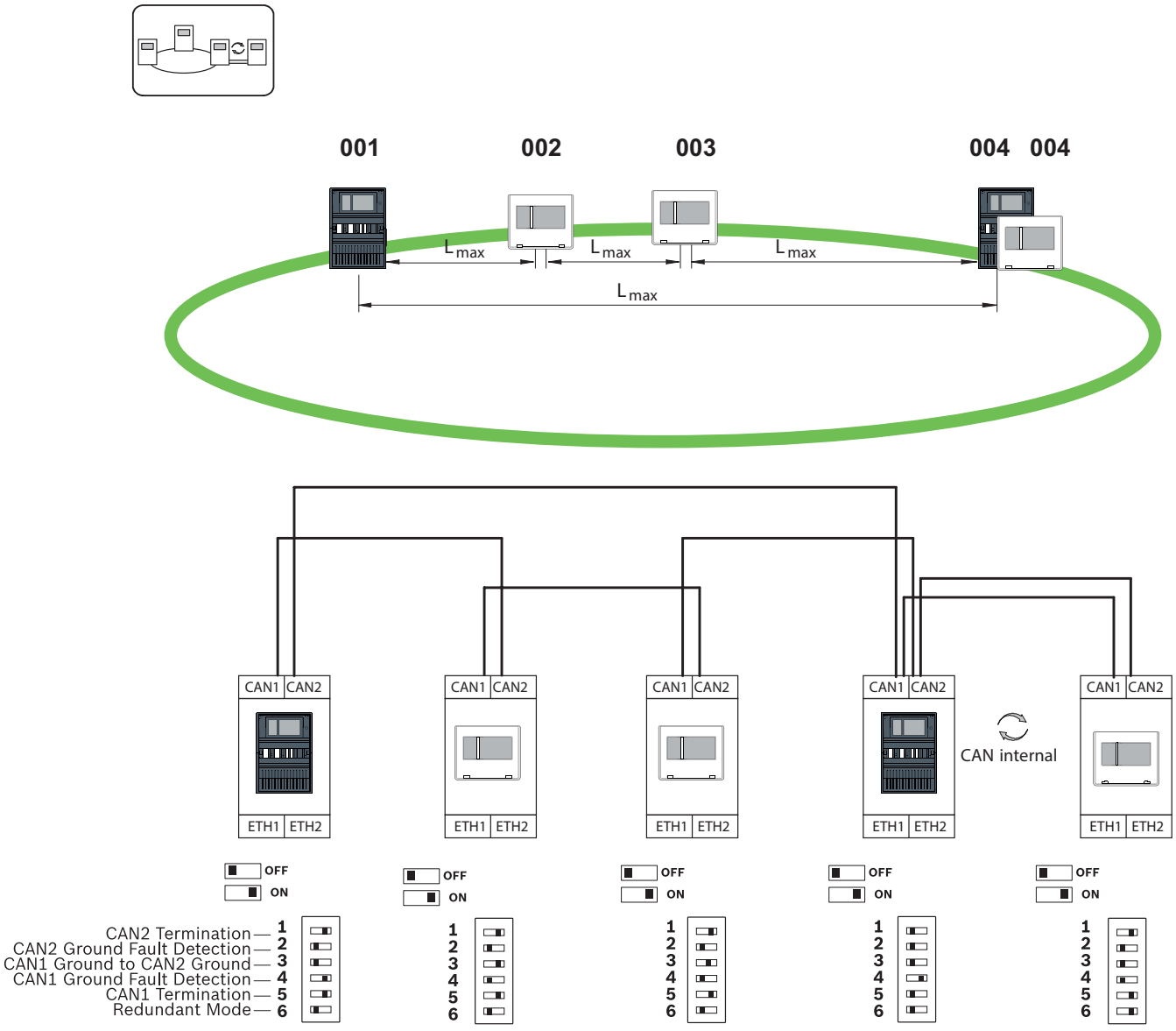


Figura 10.5: Ajustes de los conmutadores DIP para el lazo con teclado remoto (solo AVENAR)

11 Cableado

Para crear un sistema que cumpla la normativa EN 54-2, conecte los conmutadores RSTP y los conversores de medios a través de la fuente de alimentación controlada de la central de alarma de incendios.

- Para proporcionar energía a los conversores de medios y los conmutadores RSTP utilice la salida de 24 V del módulo BCM 0000 B o FPP-5000.
- Si ha conectado una fuente de alimentación redundante o va a crear una conexión de conmutador a conmutador, las salidas de avería del conmutador RSTP deben controlarse a través de las entradas de la central. Por ejemplo, utilice las entradas del controlador de la central o IOP 0008 A.
- En el caso de los conversores de medios, se debe activar la función "Link Fault Pass-Through". La configuración se realiza a través del conmutador DIP del conversor de medios.

Aviso!
Utilice solo los siguientes cables para el funcionamiento en red:
Cable Ethernet
Cable de conexión Ethernet, apantallado, CAT5e o superior.
Tenga en cuenta el radio mínimo de curvatura indicado en las especificaciones del cable.
Cable de fibra óptica
Multi modo: cable de conexión Ethernet de fibra óptica, I-VH2G 50/125µ dúplex o I-VH2G 62.5/125µ dúplex, enchufe SC.
Modo sencillo: cable de conexión Ethernet de fibra óptica, I-VH2E 9/125µ dúplex, enchufe SC.
Tenga en cuenta el radio mínimo de curvatura indicado en las especificaciones del cable.

11.1 Conversor de medios

Conexión de conversores de medio

Aviso!
Tenga en cuenta el sentido de transmisión de los cables de fibra FOC al conectar el cableado FX de los conversores de medios.

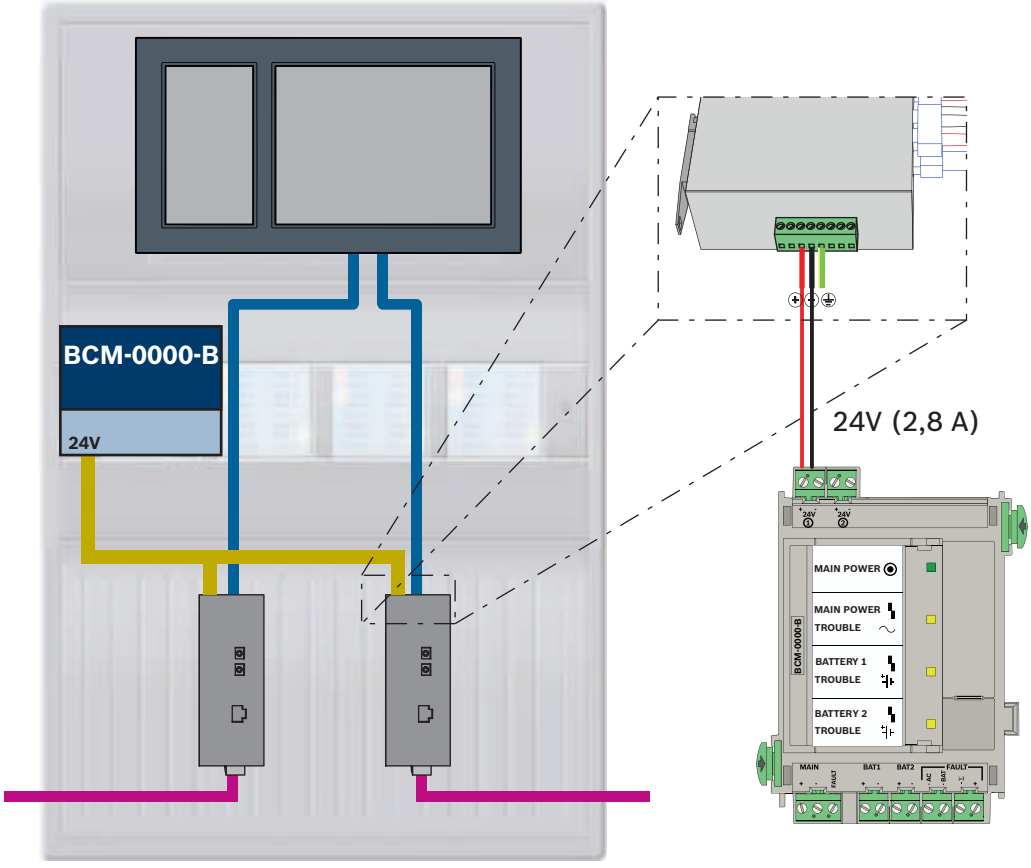


Figura 11.1: Conexión del conversor de medios a la fuente de alimentación y al controlador de la central IN1/IN2

Icono	Descripción
	Cable Ethernet TX (cobre)
	Cable Ethernet FX (cable de fibra óptica)

Icono	Descripción
	Fuente de alimentación de 24 V
	Transmisión de avería
	Conversor de medios

11.2 Switch Ethernet

Conexión del conmutador

Puede conectar las salidas de avería de los conmutados a las entradas del controlador de central o de un módulo de entrada y salida IOP.

Aviso!

El relé de avería solo se debe conectar para las aplicaciones en las que se cumpla al menos uno de los siguientes requisitos:
Existe una conexión entre 2 conmutadores. Esto ocurre en el caso de una red troncal con sublazos, por ejemplo.
La fuente de alimentación del switch se ha diseñado de manera redundante.

Conexión de los switches al notificar averías a las entradas del módulo IOP:

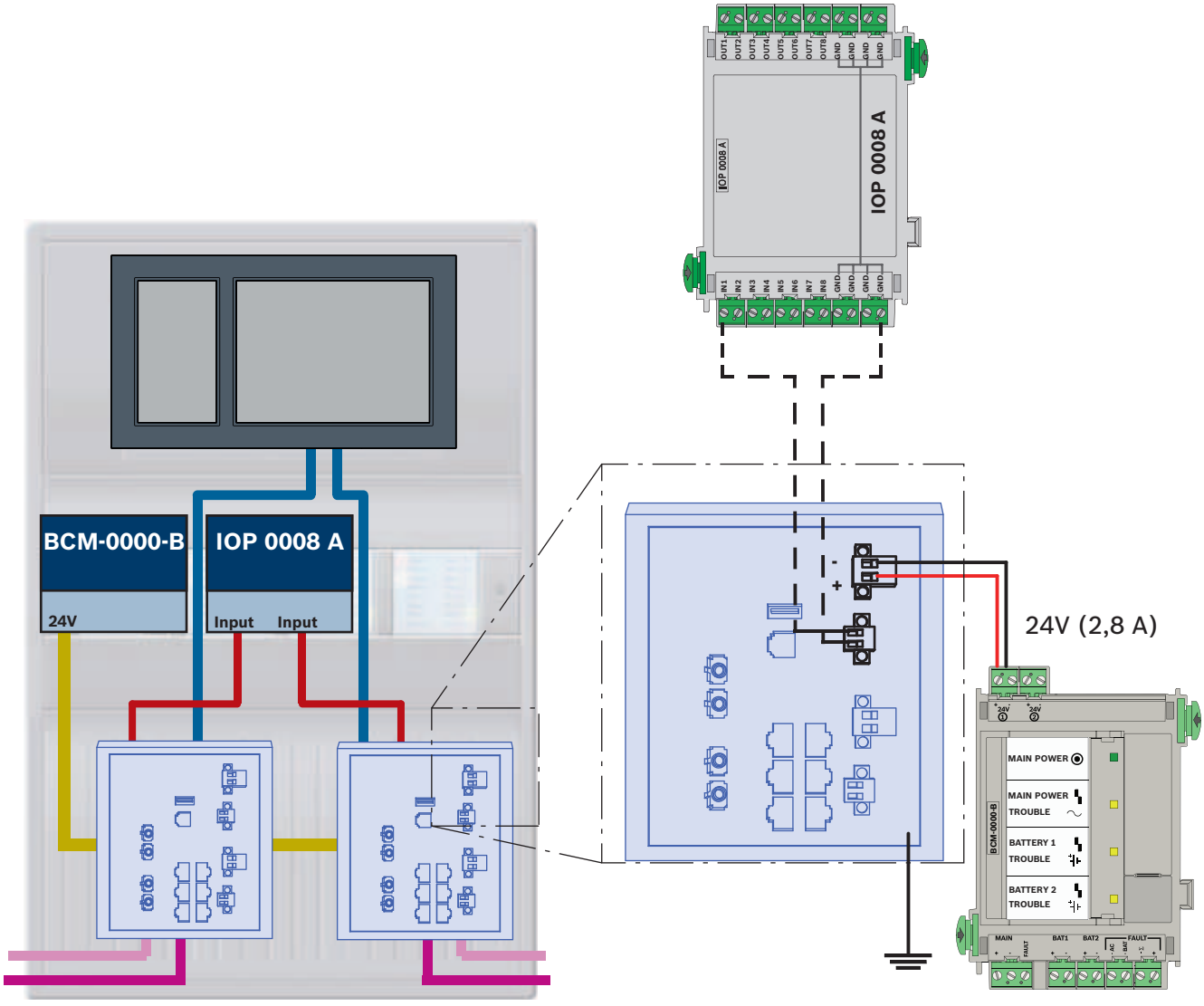


Figura 11.2: Conexión del conmutador a la fuente de alimentación e IOP

Icono	Descripción
	Cable Ethernet TX (cobre)
	Cable Ethernet FX (cable de fibra óptica)
	Fuente de alimentación de 24 V
	Transmisión de avería
	Switch RSTP

Conexión de los conmutadores con notificación de averías a las entradas del controlador de la central

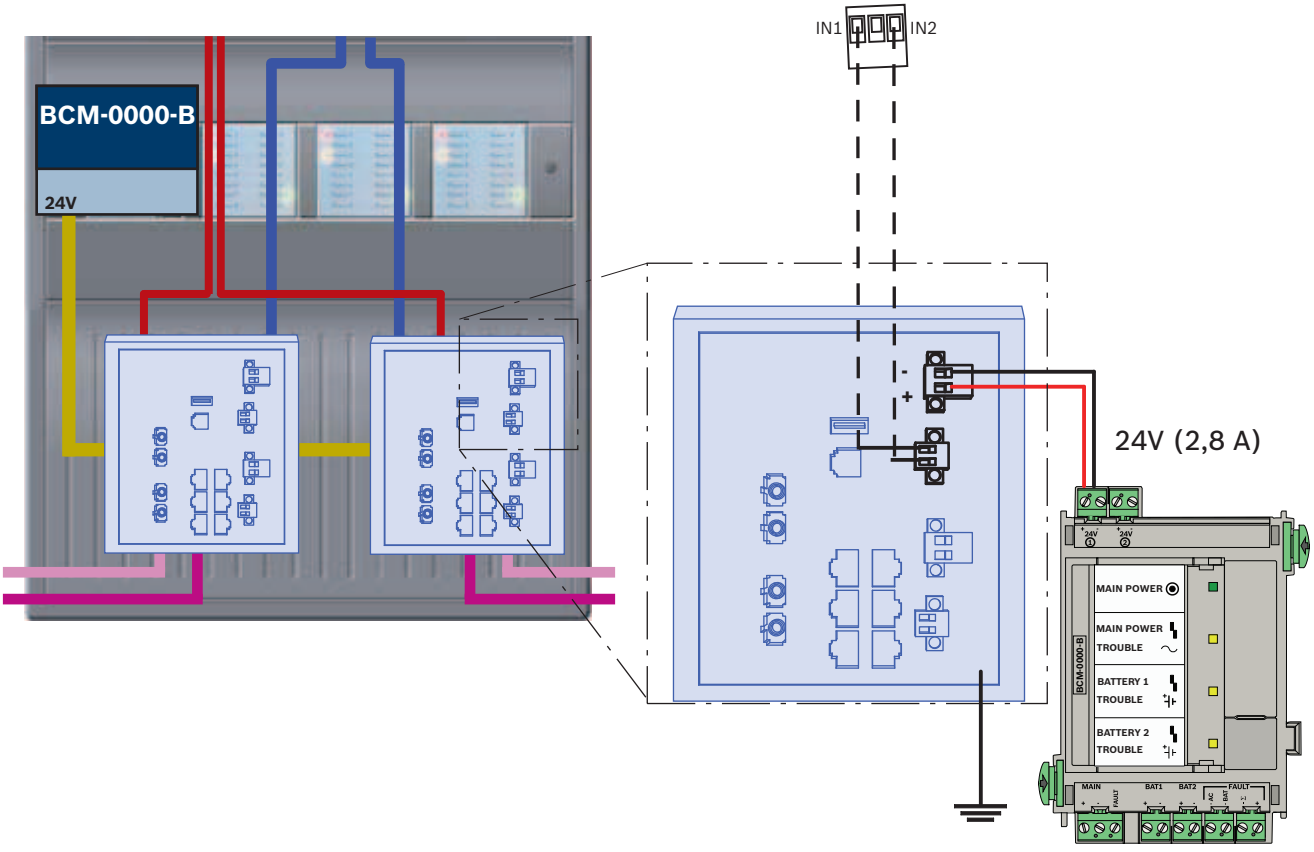
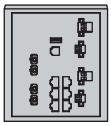


Figura 11.3: Conexión del conmutador a la fuente de alimentación y al controlador de la central

Icono	Descripción
	Cable Ethernet TX (cobre)
	Cable Ethernet FX (cable de fibra óptica)
	Fuente de alimentación de 24 V
	Transmisión de avería
	Switch RSTP

Aviso!
No utilice el cable de red suministrado para conectar los conmutadores.
Utilice un cable de conexión Ethernet, apantallado, CAT5e o superior.

11.3 Teclado remoto

Debe suministrarse un teclado remoto que reciba alimentación a través de una fuente de alimentación externa FPP-5000. La conexión a la red se establece mediante dos conversores de medios en un PSS 0002 A o un USF 0000 A.

Aviso!
Tenga en cuenta que la fuente de alimentación externa FPP-5000 y PSF 0002 A (PSS 0002 A) se deben instalar junto al teclado remoto (sin espacio intermedio). No debe ser posible que los cables de conexión de los componentes se toquen entre ellos, ya que no se supervisan para detectar cortocircuitos ni circuitos abiertos.

Aviso!
Utilice solo conversores de medios para conectar un teclado remoto a una red de centrales Ethernet.
El teclado remoto no permite el uso de switches.

Aviso!
La conexión a tierra funcional del teclado remoto debe encontrarse siempre en su posición al conectar la unidad a una red de centrales Ethernet.

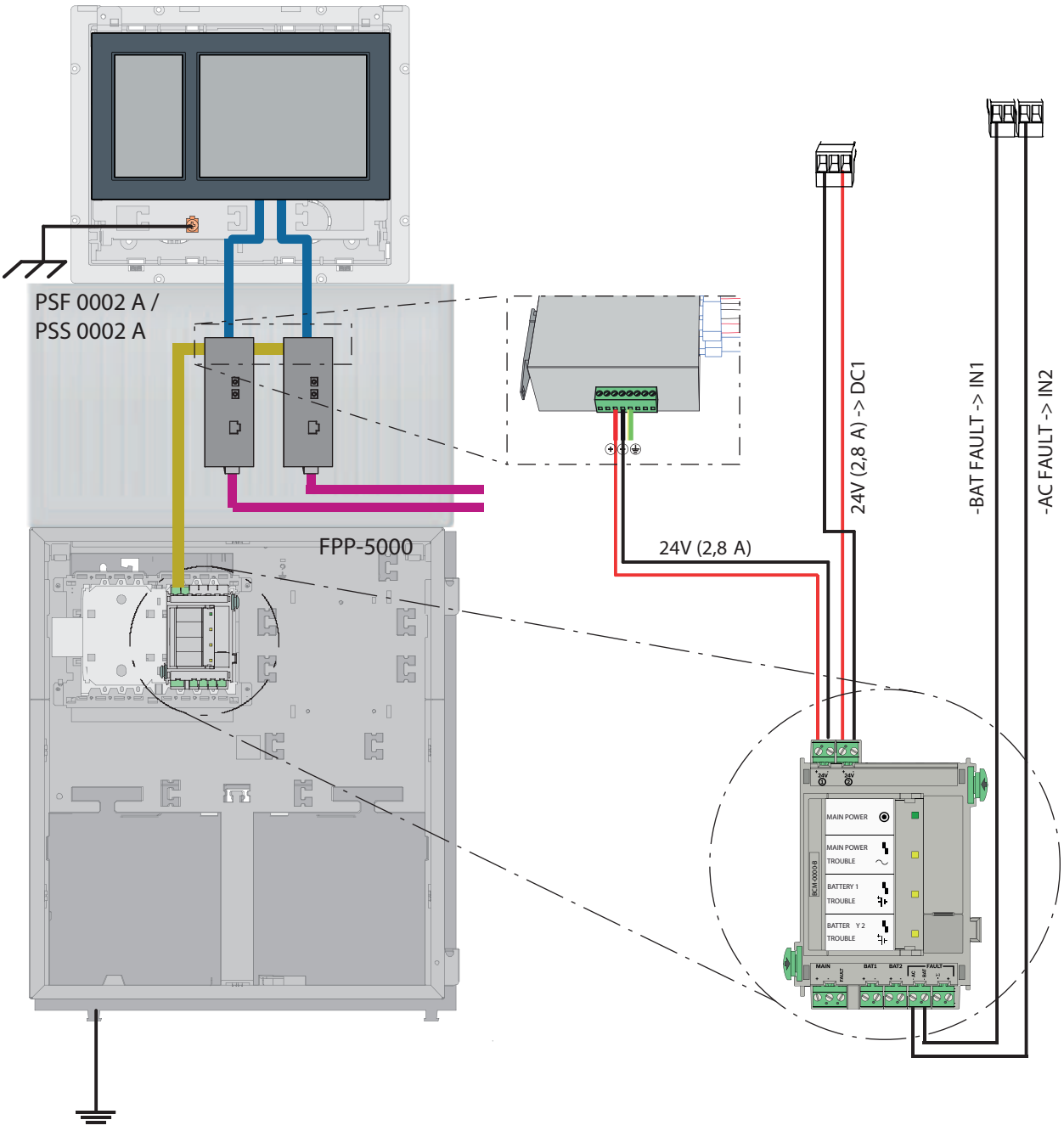


Figura 11.4: Cableado del teclado remoto

Icono	Descripción
	Cable Ethernet TX (cobre)
	Cable Ethernet FX (cable de fibra óptica)
	Fuente de alimentación de 24 V
	Conversor de medios

12 Ajustes de FSP-5000-RPS

Puede programar toda la red con el software de programación RPS a través del puerto USB, la interfaz de red o el módulo de interfaz de serie de una central. Para ello, debe configurar los ajustes de red en la central y reiniciarlos para poner en marcha la red.
De manera alternativa, también puede usar el módulo de interfaz de red de un switch que esté conectado a la red.

12.1 Nodos de red

Debe programar la red completa con todos los nodos de red en el software de programación FSP-5000-RPS y cargar todo ello en la red. Para ello, siga estos pasos:

- Conecte los nodos FPA
  - Establezca el RSN en los nodos individuales
- Ajuste el número de líneas del cableado de red para que pueda crear la topología deseada
- Compruebe la visualización de la topología para asegurarse de que es correcta
- Conecte el servidor OPC, el sistema Praesideo/PAVIRO, el servidor UGM-2040 y los switches donde sea necesario
- Edite la configuración IP y de Ethernet
  - Asigne las direcciones IP o utilice los ajustes estándar si usa una topología con menos de 20 conmutadores RSTP
  - Elija el protocolo de redundancia adecuado para la topología establecida
- Realice una comprobación
- Conéctese a la red a través de Ethernet, USB o el módulo de interfaz de serie
- Realice un inicio de sesión múltiple
- Lleve a cabo una auto detección completa para cada central
- Solicite la información de configuración y complete todas las tareas

Compruebe los mensajes de error después de reiniciar la red y corrija los errores si procede.

12.2 Números de línea

Debe asignar un número de línea a cada conexión de la red. No importa si se trata de una conexión CAN o Ethernet.
Se puede usar un número de línea para ambas conexiones, CAN y Ethernet. No obstante, para obtener una mejor perspectiva de las comunicaciones, utilice rangos de números diferentes.
Tenga en cuenta que si utiliza como en la ventana , el número de línea debe ser 0 para todas las conexiones.

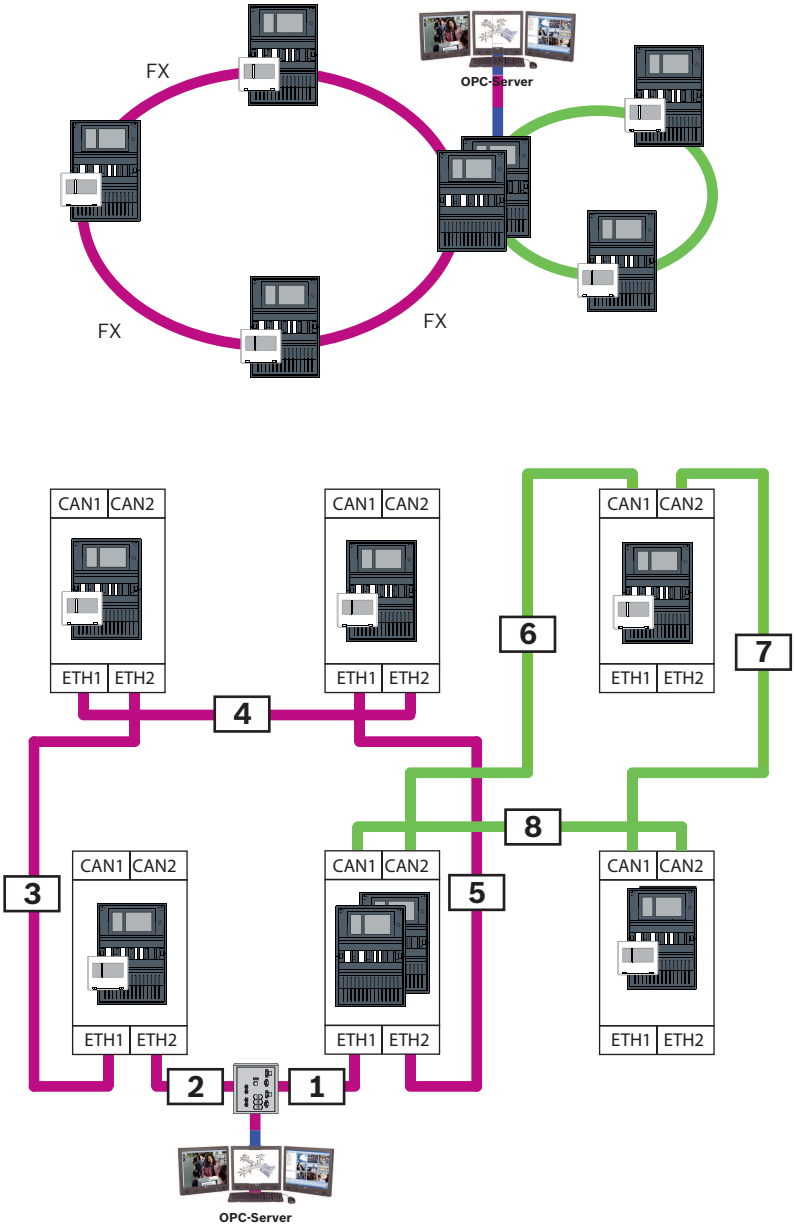


Figura 12.1: Ejemplo de una red y de la numeración de líneas posible

12.3 Conmutadores

Si utiliza switches en la red, debe crearlos en el software de programación FSP-5000-RPS. Puede asignar un máximo de 128 puertos a cada switch que cree. Para crear la red, puede asignar los números de líneas conectadas a los puertos individuales.

12.4 Servidores OPC

Es necesario añadir los servidores OPC de la red al software de programación FSP-5000-RPS. Configure los siguientes ajustes en el software FSP-5000-RPS y en el servidor OPC:

- Nodos de red
- Grupo de red
- RSN
- Dirección IP
- Puerto

El servidor OPC usa el puerto 25000 como estándar.

Aviso!
EN 54
La conexión de un sistema de gestión de edificios (p. ej., BIS) mediante una interfaz Ethernet utilizando un servidor OPC o un servidor FSI cumple con los requisitos de EN54 si la CDI realiza las funciones EN54 relevantes de forma exclusiva. Cualquier control o administración relevante para EN54 (p. ej., el control de los aparatos de notificación o la administración de la desactivación) por parte del sistema de gestión de edificios requiere una certificación EN54 específica del sistema global por parte de un organismo de certificación.

Aviso!
Software de programación FSP-5000-RPS
Debe asignar un servidor OPC a cada nodo de red cuyos estados sea necesario transmitir.

12.5 Servidores UGM-2040

Aviso!
Todos los controladores de la central y los servidores UGM se deben ubicar en la misma subred y tener la misma dirección de multidifusión.
En el caso de que haya varias configuraciones de central o redes, se deben ubicar en la misma subred. Las direcciones de multidifusión deben ser diferentes.

Aviso!
Debe asignar el servidor UGM-2040 a cada nodo de red cuyo estado se debe transmitir.

Para poder conectar una central al UGM-2040, debe simular la estructura física de la red en RPS. Esto también incluye el número de líneas entre el controlador de la central que se conecta y los conmutadores del UGM-2040.

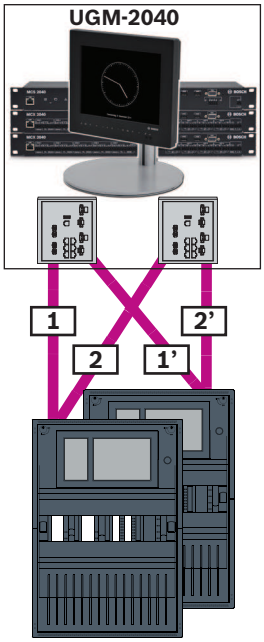


Figura 12.2: Ejemplo de numeración de líneas para el UGM-2040

13 Apéndice

13.1 Mensaje de error de Ethernet

En caso de error, se muestra el mensaje de error junto con el grupo del error para cada instancia.

Dirección física	Dirección lógica	Mensaje de error	Descripción y posible causa
Grupo de averías relacionadas con un fallo general en la red			
135.0.1.0	Red 1.0		La versión del software de red de la central no es compatible. Hay dos tipos distintos de versiones de software
Grupo de averías relacionadas con la red			
135.0.6.1	Red 2.1		Una dirección IP se ha asignado dos veces.
135.0.6.2	Red 2.2		La configuración IP de la central de notificación no coincide con la configuración de RPS.
135.0.6.3	Red 2.3		La configuración de redundancia (RSTP, parámetro RSTP, conexión dual o nothing (nada)) de la central de notificación no coincide con la configuración de RPS.
Grupo de averías relacionadas con el protocolo de árbol de expansión rápido (RSTP)			
135.0.7.1	Red 3.1		El modo de la central de notificación ha cambiado de RSTP a STP (modo de compatibilidad). Se ha conectado un dispositivo STP a la red.
135.0.7.2	Red 3.2		La topología de la red RSTP ha cambiado. Por ejemplo, se ha añadido otro dispositivo RSTP a la red. Este mensaje también puede aparecer cuando se produce una interrupción en la línea.
135.0.7.3	Red 3.3		Un puerto RSTP de la central de notificación no se encuentra en el estado de punto a punto. Por ejemplo, se han conectado varios dispositivos RSTP a un puerto RSTP. O bien, se ha conectado otro dispositivo RSTP al puerto RSTP a través de la línea de medio dúplex.
Grupo de averías relacionadas con la conexión de red			
135.0.5.1	Conexión de red 1.0		La transmisión de datos al bus CAN 1 está limitada. Algunas causas posibles son que los cables están rotos, sin conectar o con interferencias.
135.0.5.2	Conexión de red 2.0		La transmisión de datos al bus CAN 2 está limitada. Algunas causas posibles son que los cables están rotos, sin conectar o con interferencias.
135.0.5.3	Conexión de red 3.0		La transmisión de datos a la línea Ethernet 1 está limitada. Algunas causas posibles son que los cables están rotos, sin conectar o con interferencias.

Dirección física	Dirección lógica	Mensaje de error	Descripción y posible causa
135.0.5.4	Conexión de red 4.0		La transmisión de datos a la línea Ethernet 2 está limitada. Algunas causas posibles son que los cables están rotos, sin conectar o con interferencias.

Índice

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