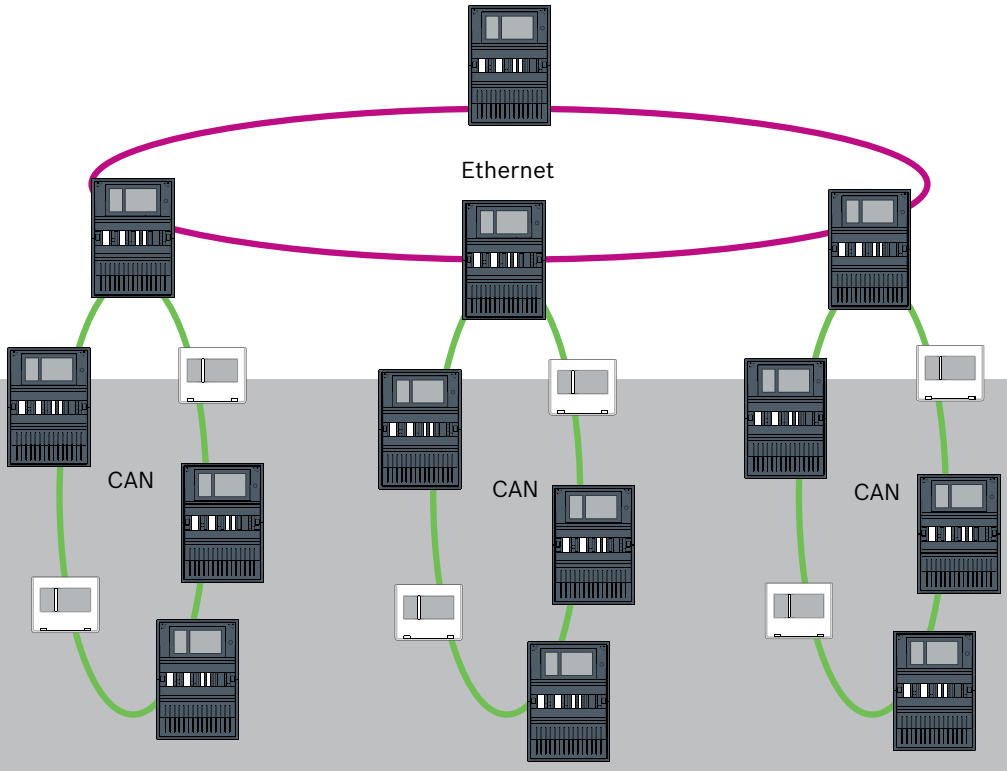
AVENAR panel | FPA-5000 | FPA-1200



pt Networking manual

Índice

1 Segurança

Este capítulo inclui as medidas organizacionais para PCs com service clients dedicados ao portefólio de produtos de incêndio da Bosch. O cumprimento destes acordos contratuais é obrigatório.
São também disponibilizados avisos de segurança compilados e ordenados por tópicos. Posteriormente, os avisos de segurança são apresentados antes das instruções relacionadas.

1.1 Medidas organizacionais para PCs com service clients

Introdução

O portefólio de produtos de incêndio da Bosch abrange os programas para PC (service clients) executados num computador que necessitem de ligação física ao sistema de alarme de incêndio. Devido às considerações de segurança e aos requisitos regulamentares padrão, o sistema de alarme de incêndio não deve ser instalado numa rede partilhada. Por sua vez, tal significa que toda a rede do sistema de alarme de incêndio e o PC com um service client devem constituir uma rede fisicamente dedicada. Dado que a Bosch apenas desenvolve os service clients e não os PCs onde estes são executados, o computador não pode ser controlado pela Bosch. Para reduzir o risco de potenciais riscos de segurança, este documento define as medidas organizacionais.

Medidas

Caso as medidas descritas abaixo necessitem de uma ligação à Internet ou o service client necessite de uma ligação temporária à Internet para fins de licenciamento, o PC deve ser fisicamente isolado da rede do sistema de alarme de incêndio antes de ser ligado à Internet. A ligação à Internet deve ser removida antes de voltar a ligar o PC à rede do sistema de alarme de incêndio.

1. Sistemas operativos
   A Bosch documenta os pré-requisitos dos service clients, incluindo as versões do sistema operativo. É garantida a compatibilidade dos clients com estas versões. O sistema operativo no qual o client é executado deve ser atualizado regularmente para fazer face a potenciais vulnerabilidades de segurança.
   O sistema deve ser configurado para permitir o acesso apenas de escrita às pastas necessárias para a tarefa correspondente. Por predefinição, todos os utilizadores devem ter permissões só de leitura.
2. Antivírus
   Deve ser instalado e executado um software antivírus de última geração no computador. Os respetivos ficheiros de definições devem ser atualizados regularmente.
3. Firewall
   O PC deve ter uma firewall de software instalada e em execução. Deve ser configurada para permitir o tráfego entre o service client e o sistema de alarme de incêndio, as atualizações do sistema operativo e o software antivírus. Adicionalmente, deve bloquear qualquer outro tipo de tráfego.
4. Início de sessão de utilizador seguro
   O acesso ao PC deve ser limitado aos operadores que utilizam o service client instalado. O início de sessão deve ser protegido por métodos de segurança avançados. Se optar por proteger o acesso através da utilização de palavra-passe, as políticas devem impor regras de palavra-passe avançadas.
   A regra de dois homens (princípio de quatro olhos) ou a autenticação multifator são abordagens recomendadas para reforçar a autenticação quando aplicável.

5. Software e serviços
   O número de programas de software instalados no PC deve ser o mínimo possível. Só deve ser instalado o software necessário ao funcionamento do service client e às tarefas correspondentes.
6. Limitações de utilização
   A utilização do PC deve ser limitada às tarefas relacionadas com o serviço através de medidas organizacionais. Isto também abrange a utilização da Internet para outros fins que não os descritos neste documento.
7. Separação de deveres
   Os deveres e as áreas de responsabilidade devem ser separados para reduzir oportunidades de modificação não autorizada ou não intencional, ou utilização incorreta; por exemplo, tarefas diferentes devem ser atribuídas a funções diferentes.
8. Monitorização
   Todas as tentativas de acesso ao PC que execute o service client devem ser monitorizadas para identificação de acessos não autorizados ao PC e à Internet.

1.2 Explicações dos símbolos de segurança

Aviso!
Indica uma situação de perigo que, caso não seja evitada, pode resultar em ferimentos graves ou morte.

Atenção!
Indica uma situação de perigo que, caso não seja evitada, pode resultar em ferimentos ligeiros ou moderados.

Informação!
Indica uma situação que, se não for evitada, pode resultar em danos no equipamento e no meio ambiente ou em perda de dados.

1.3 Avisos de segurança

Conversor de multimédia

Aviso!
Luz laser
Não olhe diretamente para o feixe tanto a olho nu como através de instrumentos de visualização de qualquer tipo (por exemplo, lupa ou microscópio). O incumprimento deste aviso representa um perigo para os olhos a uma distância inferior a 100 mm. A luz emerge nos terminais visuais ou na extremidade dos cabos de fibra ótica ligados a estes. Díodo laser CLASSE 2M, comprimento de onda 650 nm, potência < 2 mW, de acordo com a IEC 60825-1.

Remote Services

Atenção!
Para o acesso através da Internet, utilize apenas o BoschRemote Services.

Atenção!
O Remote Services necessita de uma ligação IP segura. Necessita do Remote Services da Bosch ou da ligação à Private Secure Network.
Com a Private Secure Network é fornecida uma rede IP baseada em DSL com acesso sem fios opcional no lado do painel (EffiLink). O Remote Services para a Private Secure Network só está disponível na Alemanha mediante celebração de um contrato de serviço com a Bosch BT-IE.

Informação!
Para configurar uma rede de alarme de incêndio central, é necessária uma rede Ethernet exclusiva.
A utilização de um sistema de alarme de incêndio em qualquer outra rede Ethernet é da responsabilidade do utilizador. A Bosch renuncia a qualquer garantia e responsabilidade inerentes a este tipo de utilização indevida.
Em caso de utilização de uma rede Ethernet não exclusiva, não é possível garantir a fiabilidade da transmissão do alarme nem a segurança das TI.

Ligação de segurança inteligente

Aviso!
Riscos de segurança na ligação por Ethernet
Não ligue o PRAESENSA a FPA-5000/FPA-1200 utilizando Smart Safety Link devido a riscos de segurança na ligação por Ethernet

Informação!
VdS 2540
O sistema de alarme por voz deve estar nivelado com o painel de incêndio numa única sala. Caso contrário, os requisitos de VdS 2540 para vias de transmissão de dados não são cumpridos.

Rede de painéis

Informação!
EN 54
Para garantir que a rede é configurada em conformidade com a norma EN 54, utilize apenas componentes que tenham sido aprovados para utilização em redes centrais de alarme de incêndio.
Os switches RSTP externos e os conversores multimédia nas redes Ethernet têm de ser instalados em caixas de painel. A instalação fora da caixa do painel não está em conformidade com a norma EN 54.

Informação!
Comprimento do cabo TX
Todas as ligações IP devem ser diretas ou realizadas através de conversores multimédia aprovados pela Bosch. O comprimento do cabo TX de nó a nó deve ser inferior a 100 m.

Informação!
VdS 2540
Para cumprir os requisitos de VdS 2540 para caminhos de transmissão de dados, utilize o cabo de fibra ótica para ligações Ethernet. Para ligações dentro de um compartimento, pode utilizar TX Cabos Ethernet.

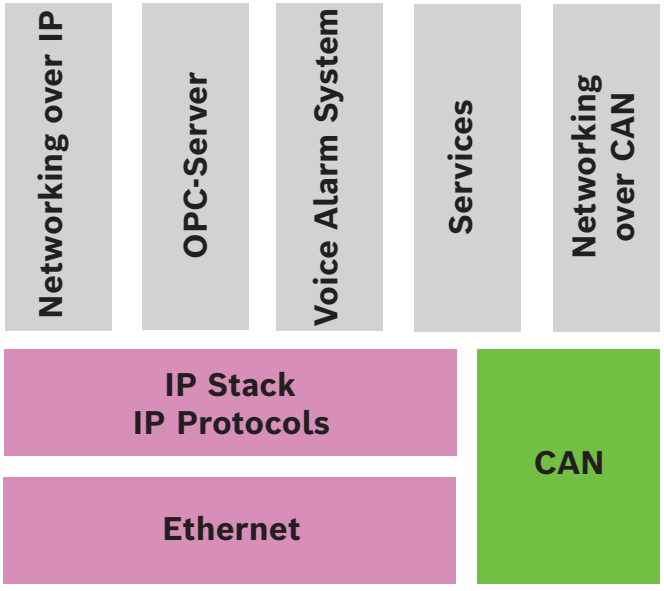
Informação!
No caso de aplicações padrão, utilize definições de rede padrão.
Só são permitidas alterações às definições de rede padrão quando são efetuadas por utilizadores experientes com conhecimentos adequados sobre ligações em rede.

Informação!
Topologias aplicáveis
A funcionalidade e a comunicação entre painéis são restringidas pelo tipo de painel. Consulte a especificação do painel para obter informações sobre serviços, o número de painéis conectáveis e o número de painéis repetidores conectáveis.

2 Introdução

Este documento destina-se a leitores com experiência de planeamento e instalação de sistemas de alarme de incêndio em conformidade com a norma EN 54. São também necessários conhecimentos de ligação em rede.
Este documento descreve as diversas topologias de rede de alarme de incêndio. As topologias são descritas de forma independente do tipo de painel de incêndio.
Para criar redes de painel correspondentes às topologias e aos serviços de ligação introduzidos, necessita do padrão de ligação em rede descrito neste documento.
O documento fornece uma descrição geral das condições básicas, dos valores limite e dos procedimentos gerais de projeto e instalação da rede de painéis.
É possível encontrar descrições detalhadas da instalação de componentes individuais nos respetivos manuais de instalação.
Existe uma descrição da interface do utilizador do painel de controlo no manual de operação fornecido com o dispositivo.
A interface do utilizador do software de programação FSP-5000-RPS é descrita na ajuda online.

3 Vista geral do sistema



Na rede, a interface Ethernet e os protocolos IP são utilizados em serviços diferentes. A interface Ethernet pode ser completamente desativada ou a sua utilização pode ser desativada apenas para a ligação em rede através de TCP/IP. A desativação poderá ser necessária para a ligação em rede através de CAN.

Ativação de serviços

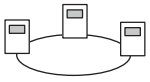
- ligação em rede através de TCP/IP
  No FSP-5000-RPS, ative a comunicação painel a painel na rede Ethernet
- Servidores OPC
  Adicione um servidor OPC à configuração FSP-5000-RPS
- Ligação ao Sistema de Alarme por Voz
  Adicione um Sistema de alarme por voz à configuração FSP-5000-RPS e configure disparos virtuais.
- Remote Services (Remote Connect como pré-requisito, Remote Maintenance e Remote Alert)
  Ative a caixa de verificação relevante no FSP-5000-RPS
- Remote Services (Remote Connect como pré-requisito, Remote Maintenance e Remote Alert) para Private Secure Network
  Adicione o acesso remoto à configuração FSP-5000-RPS e configure o acesso remoto no FSP-5000-RPS.

Informação!
Transferência de dados não intencional
Se a interface Ethernet do painel de controlo se destinar a ser utilizada apenas para comunicar com um servidor OPC ou para o Remote Services, desative a comunicação entre painéis através de TCP/IP no FSP-5000-RPS. Caso contrário, os dados de incêndio podem ser transferidos inadvertidamente através da Ethernet.

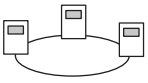
Para operar serviços baseados em Ethernet ou em TCP/IP, as interfaces Ethernet têm de ser ativadas e têm de ser configuradas as definições TCP/IP corretas.

Rede de painéis e painéis repetidores

A tabela apresenta as opções para ligação em rede de painéis/painéis repetidores consoante a topologia da rede e o tipo de painel. Tenha em conta os limites determinados pela topologia da rede.

Topologia	**AVENAR panel 8000, licença premium**	**AVENAR panel 8000, licença standard**	**AVENAR panel 2000, licença premium**	**AVENAR panel 2000, licença standard**
 Autónomo	Possível	Possível	Possível	Possível
 Loop	Máx. de 32 painéis/painéis repetidores, conectividade com AVENAR panel 2000, licença premium e FPA	Máx. de 32 painéis/painéis repetidores, conectividade com AVENAR panel 2000, licença premium e FPA	Máx. de 32 painéis/painéis repetidores, conectividade com AVENAR panel 8000 e FPA	Painel 1 e máx. de 3 painéis repetidores
 Redundância de painel	O painel de controlo redundante também deve ser premium. Também pode	O painel de controlo redundante pode ser standard. Também pode utilizar um painel	Impossível	Impossível

Topologia	**AVENAR panel 8000, licença premium**	**AVENAR panel 8000, licença standard**	**AVENAR panel 2000, licença premium**	**AVENAR panel 2000, licença standard**
	utilizar um painel repetidor como painel redundante.	repetidor como painel redundante.		

Topologia	**FPA-5000**	**FPA-1200**
 Autónomo	Possível	Possível
 Loop	Máx. de 32 painéis e painéis repetidores	Painel 1 e máx. de 3 painéis repetidores
 Redundância de painel	Possível	Impossível (o DIP 6 no painel de controlo não está operacional.)

Se expandir uma rede FPA-5000, a Bosch recomenda que realize a expansão com um painel da série AVENAR panel.
Se trocar um painel da série FPA por um painel da série AVENAR panel, só tem de trocar o painel de controlo. Lembre-se de que os painéis da série AVENAR panel não suportam cartões de endereços. Caso exista um switch Ethernet ligado, pode continuar a utilizá-lo.
Se trocar um painel repetidor da série FPA por um painel repetidor da série AVENAR panel, verifique se a resistência da linha está dentro do intervalo especificado para o painel repetidor da série AVENAR panel.

Informação!
Instalação de firmware
Os painéis ligados devem ter a mesma versão de firmware.
Só é possível efetuar uma instalação de firmware para o painel ativo. Para painéis redundantes, instale o firmware em ambos os painéis. Para tal, tem de desligar as funções do painel e voltar a ligá-las após a instalação com êxito do firmware.

Informação!
Versões de Firmware
Para um sistema contendo exclusivamente nós AVENAR, é recomendado executar a última versão de firmware de painel 4.x.
Para um sistema contendo pelo menos um nó FPA/FMR, é recomendado executar a última versão de firmware de painel 3.x.

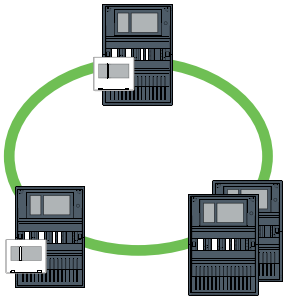
Informação!
De 1 de janeiro de 2022 a 31 de dezembro de 2025, a versão 3.x do firmware do painel está em modo de manutenção. Durante este período, serão lançadas novas versões contendo correcções para bugs críticos e falhas de segurança críticas. Não estão planeadas novas características do produto, dispositivos periféricos LSN, idiomas GUI e alterações normativas a serem adicionadas.
Após 31 de dezembro de 2025, a execução de firmware V3.x em painéis que estão ligados a uma interface Ethernet ou rede aumenta os riscos de segurança. É fortemente recomendada a realização de uma avaliação de risco de segurança. Quando os riscos de segurança são identificados, é obrigatório atualizar para AVENAR panel e executar o firmware V4.x mais recente.

Informação!
Painel de controlo redundante
Não é possível combinar um painel de controlo da série AVENAR panel e um painel de controlo da série FPA para fins de redundância.

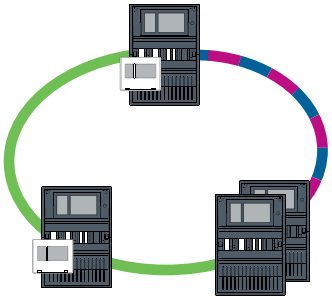
4 Topologias

Este documento descreve as diversas topologias de rede de alarme de incêndio. As topologias são descritas de forma independente do tipo de painel de incêndio.

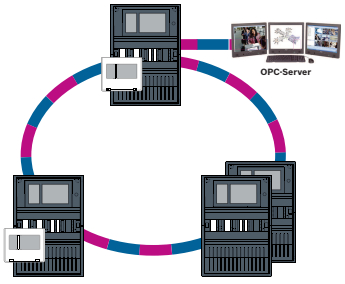
Informação!
Topologias aplicáveis
A funcionalidade e a comunicação entre painéis são restringidas pelo tipo de painel. Consulte a especificação do painel para obter informações sobre serviços, o número de painéis conectáveis e o número de painéis repetidores conectáveis.



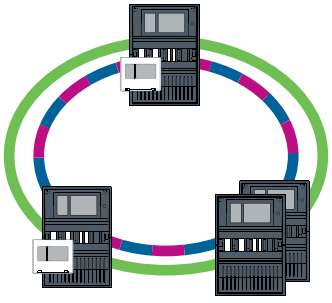
Loop CAN, página 16



Loop CAN com segmentos Ethernet, página 18

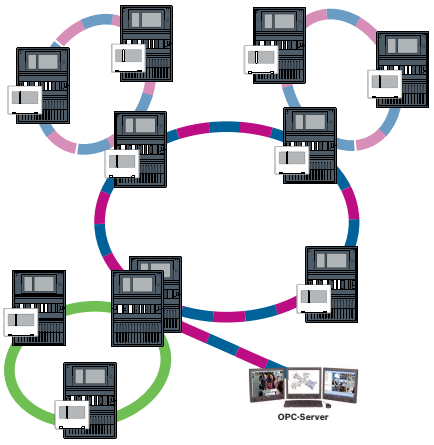


Loop Ethernet, página 16
Loop Ethernet com servidor OPC, página 17

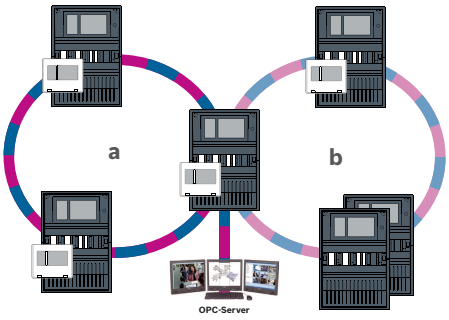


Loop duplo Ethernet/CAN, página 18

Loop Ethernet com servidor OPC para painel redundante, página 17

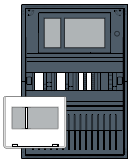
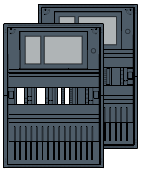
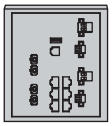


Infraestrutura Ethernet com subloops (Ethernet/CAN), página 18



Ligação de loops Ethernet, página 20

Cabo	Descrição
	TX Cabo Ethernet (cobre), comprimento do cabo TX de nó a nó < 100 m
	Cabo Ethernet FX (cabo de fibra ótica)
	Cabo Ethernet TX ou FX, comprimento do cabo TX de nó a nó < 100 m
	Cabo CAN, comprimento do cabo CAN de nó a nó < 1000 m

Dispositivo	Descrição
	Painel ou painel repetidor (na topologia Ethernet, um switch RSTP interno cada)
	Painel ou painel redundante (em switch RSTP interno de topologia Ethernet) Um painel repetidor pode ser utilizado como painel de controlo redundante. As ligações de rede e as definições são idênticas para um painel de controlo redundante e um teclado redundante. A utilização de um teclado redundante é aplicável apenas a AVENAR panel 8000.
	Switch Ethernet como switch RSTP externo (em geral, switch Ethernet MM)
	Conversor de multimédia

Dispositivo	Descrição
	Gateway de rede segura para Remote Services

Limites da rede

O número de painéis e painéis repetidores que podem ser ligados em rede depende da escolha da topologia da rede.

Os painéis e os painéis repetidores ligados em rede são conhecidos como nós.

– O número de pontos de deteção numa rede está limitado a 32768.
– O número de pontos de deteção por painel operado numa rede está limitado a 2048.
– O número de nós por sistema depende do tipo de topologia.
  Um nó pode ser um painel de controlo ou um painel repetidor.
– O número de nós numa topologia em loop está limitado a 32.
– O FSP-5000-RPS permite atribuir um máximo de 3 painéis repetidores configurados a um painel.

A cablagem entre os nós e o comprimento máximo do cabo permitido também são determinados pela escolha da topologia.

É possível combinar até 32 painéis de controlo, painéis repetidores e servidores OPC de modo a formar uma rede.

Consoante a aplicação pretendida, os diferentes painéis de controlo e painéis repetidores podem ser divididos em grupos e definidos como nós de rede ou nós locais. Em regra, num determinado grupo, só é possível visualizar o estado dos painéis de controlo pertencentes ao grupo definido. O estado de todos os painéis de controlo pode ser apresentado e/ou processado a partir de nós da rede, independentemente do grupo a que os painéis pertençam.

Endereço de nó físico

Um painel ou um painel repetidor é identificado na rede por um endereço exclusivo denominado endereço de nó físico.

Informação!

Endereço de nó físico para painéis redundantes

Um painel redundante deve ter o mesmo endereço de nó físico que o painel principal atribuído.

Informação!

A rede utilizada tem de cumprir os seguintes requisitos mínimos:

Saída mínima: 1 Mbps

Latência máxima: 250 ms

Informação!

EN 54

Para garantir que a rede é configurada em conformidade com a norma EN 54, utilize apenas componentes que tenham sido aprovados para utilização em redes centrais de alarme de incêndio.

Os switches RSTP externos e os conversores multimédia nas redes Ethernet têm de ser instalados em caixas de painel. A instalação fora da caixa do painel não está em conformidade com a norma EN 54.

Informação!
Painel redundante - EN 54-2
De acordo com a norma EN 54-2, é possível ligar um máximo de 512 pontos de deteção para cada painel. Se este número for excedido, tem de projetar o painel de uma forma redundante. Adicionalmente, se um painel agir como uma interface com um subloop CAN e existirem mais de 512 pontos de deteção ligados no subloop, terá de projetar o painel de forma redundante. O switch RSTP que liga os 2 loops realiza a redundância.
Para um painel autónomo, pode ligar um máximo de 4096 pontos de deteção, mesmo que tenha sido projetado de forma redundante. Se o painel estiver incluído numa rede, pode ligar um máximo de 2048 pontos de deteção.

Informação!
Certifique-se de que o endereço de nó físico atribuído ao painel corresponde ao especificado no software de programação. Este último é responsável pela definição do último número do endereço IP nas definições padrão.
Ative o RSTP como protocolo de redundância e adote os valores padrão predefinidos.

Definições padrão da Ethernet do painel de incêndio
Nas definições padrão do painel de incêndio, o software de programação FSP-5000-RPS e a unidade de controlo adotam o endereço de nó físico definido como o último número do endereço IP.

Informação!
A definição correta do endereço de nó físico nos painéis de controlo e no software de programação FSP-5000-RPS é um requisito para que a rede funcione adequadamente.

Informação!
A utilização da redundância da Ethernet tem de ser ativada em separado no painel de controlo.

- Definições de IP
  - Endereço IP 192.168.1.x
    O último dígito do endereço IP nas definições padrão é sempre idêntico ao endereço de nó físico definido no painel de controlo.
  - Ecrã de rede 255.255.255.0
  - Gateway 192.168.1.254
  - Endereço multicast 239.192.0.1
  - Número da porta 25001 - 25008 (só pode ser definida a primeira porta, são sempre utilizadas 8 portas consecutivas)
- Parâmetros RSTP (predefinições)
  - Bridge Priority 32768
  - Hello Time 2
  - Max. Age 20
  - Forward Delay 15

Informação!
Pode utilizar as definições padrão da configuração IP com redes que incluam até 20 switches RSTP.
No caso de redes com mais de 20 switches RSTP, são necessárias definições adicionais consoante a topologia. É necessário um conhecimento aprofundado das redes.

Definições para loops com mais de 20 switches RSTP
Se existirem mais de 20 switches RSTP na rede, tem de ajustar as definições RSTP no painel de controlo e no software de programação. Os painéis de controlo, os painéis repetidores e os switches RSTP externos ligados são categorizados como switches RSTP. Os painéis de controlo redundantes não são considerados switches RSTP, uma vez que o switch aí contido não funciona como switch RSTP.

- Parâmetros de RSTP
  - Mantenha Bridge Priority 32768
  - Mantenha Hello Time 2
  - Altere Max. Age de 20 para 40
  - Altere Forward Delay de 15 para 25

Parâmetros
- Podem ser utilizados, no máximo, 32 nós num loop.
- O diâmetro da rede não pode ser superior a 32; consulte *Diâmetro da rede, página 23*.
- Os switches Ethernet não devem ser utilizados fora das caixas de painel.
- Os conversores multimédia não devem ser utilizados fora das caixas de painel.

Características
- A rede está em conformidade com a norma EN 54.
- A rede utiliza RSTP.

Ligação ao BIS com servidor OPC
Quando efetuar a ligação a um sistema de gestão de edifícios (BIS) através de um servidor OPC e Ethernet 100BaseTX em múltiplas redes de edifícios, é necessário esclarecer com o administrador de rede se:

1. A rede foi projetada para ligar vários edifícios? (por exemplo, não deve existir interferência técnica devido a diferenças nos potenciais de ligação à terra)
2. A largura de banda dos utilizadores do bus é suficiente para a rede?

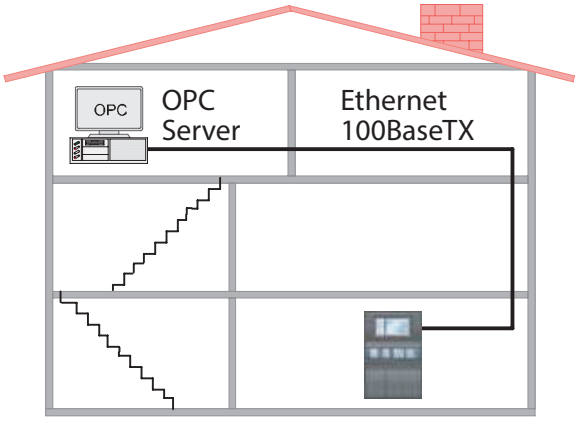


Figura 4.1: Ligação ao BIS através do servidor OPC

Informações adicionais ao utilizar um servidor OPC
Os servidores OPC da sua rede devem ser adicionados ao software de programação FSP-5000-RPS.

Tem de efetuar as seguintes definições tanto no software FSP-5000-RPS como no servidor OPC:

- Nós de rede
- Grupo de rede
- RSN
- Endereço IP
- Porta

O servidor OPC utiliza a porta 25000 como padrão.

Informação!
EN 54
A ligação de um sistema de gestão de edifícios (por exemplo, BIS) através de uma interface Ethernet com um servidor OPC ou um servidor FSI cumpre os requisitos da norma EN54 desde que as funções relevantes da EN54 sejam realizadas apenas pelo painel de incêndio. Qualquer controlo ou administração relevante da EN54 (por exemplo, controlo de aparelhos de notificação ou administração de desativação) pelo sistema de gestão de edifícios requer uma certificação EN54 individual do sistema em geral por um organismo de certificação.

Informação!
Software de programação FSP-5000-RPS
Tem de atribuir um servidor OPC a cada nó da rede a partir do qual os estados devem ser transmitidos.

4.1 Loop CAN

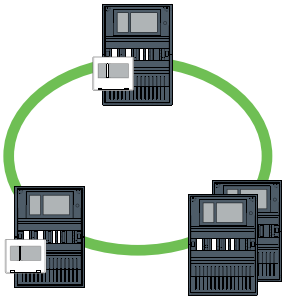


Figura 4.2: Loop CAN

4.2 Loop Ethernet

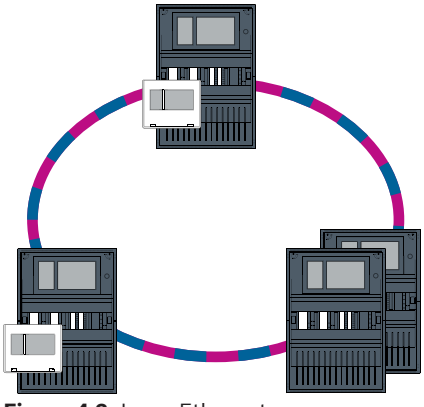


Figura 4.3: Loop Ethernet

4.3 Loop Ethernet com servidor OPC

O switch Ethernet para ligação do servidor OPC tem de ser programado em separado.
Programe o endereço IP e as definições de redundância do switch Ethernet; consulte *Definições do interruptor, página 51*. Como o switch é instalado nas proximidades imediatas (sem espaço intermédio), a fonte de alimentação não tem de ser projetada de forma redundante e as saídas de falha não são consequentemente utilizadas.
Certifique-se de que as definições de RSTP nos painéis de controlo, no FSP-5000-RPS e no switch Ethernet são idênticas.

O servidor OPC tem de ser programado em separado
Programe o endereço IP, os nós de rede, o grupo de rede e o RSN. Consulte a secção correspondente no capítulo Instalação do Manual de ligação em rede.
O servidor OPC utiliza a porta 25000 por padrão.
Certifique-se de que as definições no software de programação FSP-5000-RPS e no servidor OPC são idênticas.

Parâmetros

– O servidor OPC pode ser ligado através de um cabo Ethernet (cobre) ou através de um cabo de fibra ótica.

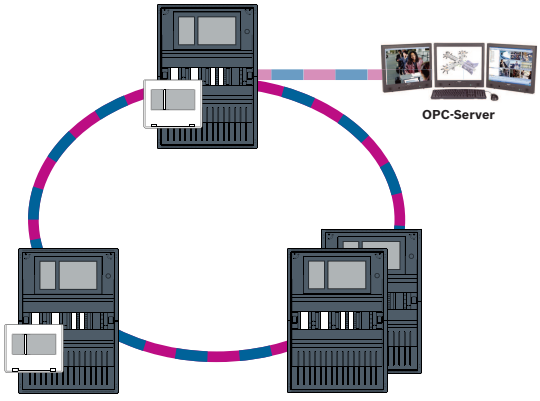


Figura 4.4: Loop Ethernet com servidor OPC

4.4 Loop Ethernet com servidor OPC para painel redundante

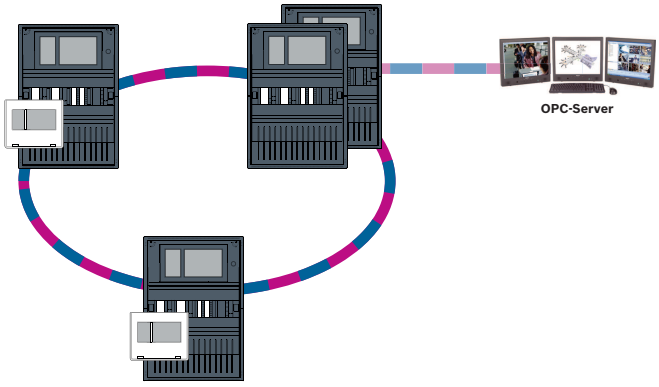


Figura 4.5: Loop Ethernet com servidor OPC para painel redundante

4.5 Loop duplo Ethernet/CAN

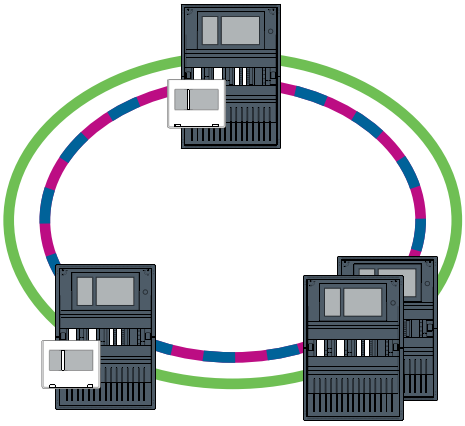


Figura 4.6: Loop duplo da Ethernet e CAN

4.6 Loop CAN com segmentos Ethernet

A topologia principal é um loop CAN. Quando a distância entre dois nós é superior a 1000 m, pode ser utilizada uma ligação FX Ethernet para cobrir a distância.

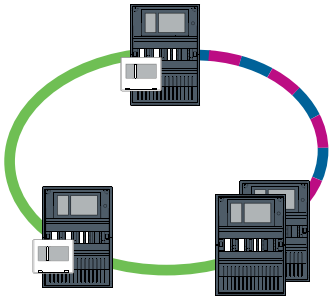


Figura 4.7: Loop CAN com segmentos Ethernet

4.7 Infraestrutura Ethernet com subloops (Ethernet/CAN)

Uma infraestrutura Ethernet está ligada a todos os subloops e, consequentemente, a uma área principal com elevadas velocidades de transmissão de dados. Por predefinição, os switches RSTP da infraestrutura não são superordenados. Tenha em atenção que, com esta topologia, é necessário determinar o diâmetro da rede. Os painéis de controlo, os painéis repetidores e os switches RSTP externos ligados são categorizados como switches RSTP. Os painéis CAN em rede não são contemplados na determinação do diâmetro da rede.
Considere as definições de loops com mais de 20 switches RSTP; consulte *Definições para loops com mais de 20 switches RSTP, página 15*.

Informação!
Esta topologia exige definições adicionais para todos os switches RSTP na infraestrutura. Por conseguinte, são necessários conhecimentos mais aprofundados sobre redes.

Informação!
De acordo com a norma EN 54-2, se o painel funcionar como uma interface com um subloop CAN, este painel tem de ser concebido de uma forma redundante se forem ligados mais de 512 pontos de deteção no subloop.
Esta restrição não se aplica num subloop Ethernet, uma vez que os interruptores que ligam os dois loops criam a redundância.

Definições adicionais

Tem de utilizar o loop central como infraestrutura. Este loop central tem de ser ligado em rede através da Ethernet.

Informação!

Para todos os switches RSTP na infraestrutura, defina uma prioridade RSTP superior à definida nos subloops. Isso garante que a ponte raiz RSTP irá permanecer sempre na infraestrutura, mesmo que haja uma falha.
Os switches RSTP para a ligação dos loops são parte da infraestrutura!
Utilize uma prioridade RSTP de 16384 na infraestrutura.

Informação!

Quanto menor for o valor definido, maior será a prioridade RSTP.

Os switches para ligação do servidor OPC e os subloops têm de ser programados em separado

Programe o endereço IP e as definições de redundância dos switches Ethernet; consulte *Definições do interruptor, página 51*. Nesta topologia, as saídas de falha do switch só têm de ser utilizadas se tiver projetado a alimentação do switch de forma redundante ou se existir uma ligação switch a switch; consulte *Switch Ethernet, página 62*.
Certifique-se de que as definições de RSTP nos painéis de controlo, no FSP-5000-RPS e no switch Ethernet são idênticas.

Informação!

Altere a prioridade RSTP dos switches RSTP que ligam os loops, uma vez que estes pertencem à infraestrutura.

O servidor OPC tem de ser programado em separado.

Programe o endereço IP, os nós de rede, o grupo de rede e o RSN; consulte *Servidores OPC, página 68*.
O servidor OPC utiliza a porta 25000 por padrão.
Certifique-se de que as definições no software de programação RPS e no servidor OPC são idênticas.

Parâmetros

– O servidor OPC pode ser ligado através de um cabo Ethernet (cobre) ou através de um cabo de fibra ótica.

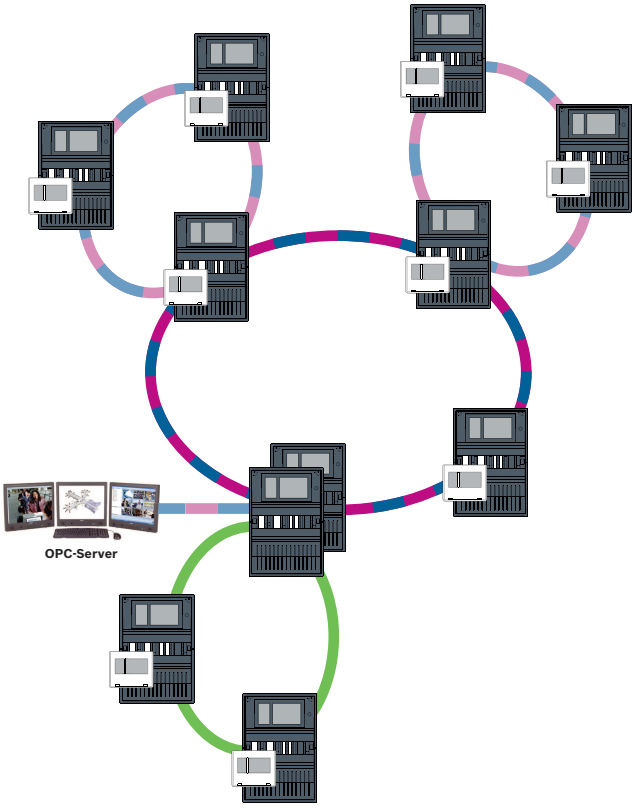


Figura 4.8: Infraestrutura Ethernet com subloops

4.8 Ligação de loops Ethernet

Informação!
Esta topologia exige definições adicionais para todos os switches RSTP na infraestrutura. Por conseguinte, são necessários conhecimentos mais aprofundados sobre redes.

Definições adicionais
Esta topologia é uma instância especial da infraestrutura Ethernet com subloops; consulte Infraestrutura Ethernet com subloops (Ethernet/CAN). Tem de utilizar um dos dois loops como infraestrutura.

Informação!
Em todos os painéis e switches na infraestrutura, defina uma prioridade RSTP superior à definida nos subloops. Isso irá garantir que a ponte raiz RSTP irá permanecer sempre na infraestrutura, mesmo que haja uma falha.
Os switches para a ligação dos dois loops são parte da infraestrutura!
Utilize uma prioridade RSTP de 16384 na infraestrutura.

Informação!
Quanto menor for o valor definido, maior será a prioridade RSTP.

Os switches para a ligação do servidor OPC e do segundo loop têm de ser programados em separado

Programe o endereço IP e as definições de redundância do switch Ethernet; consulte *Definições do interruptor, página 51*. Nesta topologia, as saídas de falha do switch só têm de ser utilizadas se tiver projetado a alimentação do switch de forma redundante; consulte *Switch Ethernet, página 62*.

Certifique-se de que as definições de RSTP nos painéis de controlo, no FSP-5000-RPS e no switch Ethernet são idênticas.

Altere a prioridade RSTP dos switches para a ligação dos dois loops, uma vez que pertencem à infraestrutura.

O servidor OPC tem de ser programado em separado

Programe o endereço IP, os nós de rede, o grupo de rede e o RSN. Consulte a secção correspondente no capítulo Instalação do Manual de ligação em rede.

O servidor OPC utiliza a porta 25000 por padrão.

Certifique-se de que as definições no software de programação FSP-5000-RPS e no servidor OPC são idênticas.

Parâmetros

– O servidor OPC pode ser ligado através de um cabo Ethernet (cobre) ou através de um cabo de fibra ótica.

Nestes exemplos, o loop a é a infraestrutura. O loop b é o subloop.

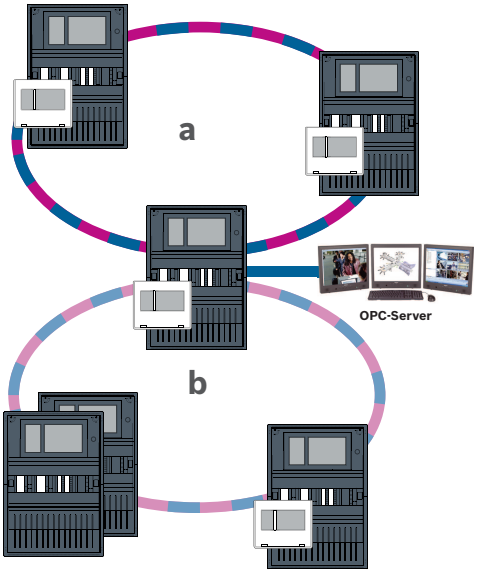


Figura 4.9: Ligação do loop Ethernet através de um painel não redundante

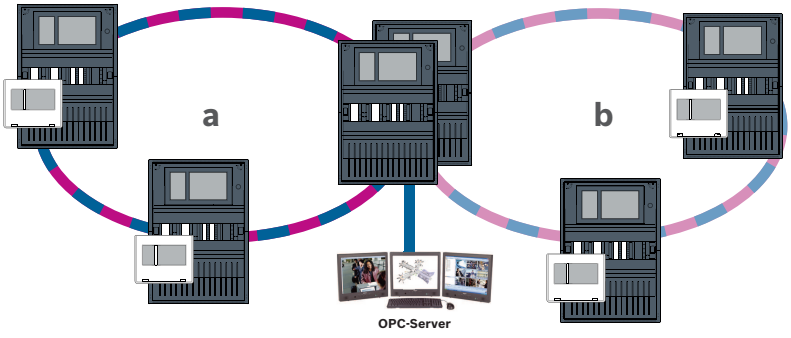


Figura 4.10: Ligação do loop Ethernet através de um painel redundante

5 Rede Ethernet

Na rede, as ligações de rede Ethernet são monitorizadas continuamente. Se uma ligação for interrompida, então a interrupção será detetada. As ligações reparadas também são detetadas. O diagnóstico de rede do painel apresenta sempre o endereço MAC dos anfitriões ligados através da rede.

Endereços MAC

Para a ligação de rede, cada painel de controlo fornece os seguintes endereços MAC.

– Endereço MAC para o anfitrião
– Endereço MAC para identificar a porta ETH1
– Endereço MAC para identificar a porta ETH2

Dependendo do tipo do painel de controlo:

– Endereço MAC para identificar a porta ETH3
– Endereço MAC para identificar a porta ETH4

Regras para a utilização de 4 portas Ethernet

Se o seu painel tiver 4 portas Ethernet, aplique as seguintes regras pela ordem indicada. A Bosch apenas suporta redes criadas de acordo com as regras a seguir.

1. Para a ligação em rede dos painéis, tem de utilizar ETH1 e ETH2. Um switch RSTP externo em ETH1 ou ETH2 só deve ser utilizado para a ligação em rede dos painéis.
2. Para ligar um OPC, um FSM-5000-FSI, um Sistema de alarme por voz, um UGM-2040 tem de utilizar ETH3. Pode ligar um switch RSTP externo que não deve ser utilizado para a ligação em rede dos painéis.
3. Para Remote Services, tem de utilizar ETH4. Se não houver ligação a Remote Services é necessário, então ETH4 pode ser usado para ligar um OPC, um FSM-5000-FSIum Sistema de alarme por voz, ou um UGM-2040.
4. Se não houver uma rede de painéis através de ETH1 e ETH2cada um pode ser utilizado para ligar um OPC, um FSM-5000-FSIum Sistema de alarme por voz, ou um UGM-2040.

5.1 Protocolos

SNMP

O protocolo SNMP é utilizado para monitorizar e controlar os componentes de rede. Para o fazer, é possível ler e modificar os parâmetros dos nós da rede. Para isso, é necessário software de gestão de rede adequado (por exemplo, o Hirschmann HiVision).

Informação!

A rede utiliza a cadeia de carateres de comunidade SNMP fixa: PUBLIC

Tenha em conta que a série AVENAR panel ainda não suporta o protocolo SNMP.

LLDP

O LLDP é um protocolo básico em conformidade com a norma IEEE e é utilizado para partilhar informações de rede entre dispositivos adjacentes. Estas informações são

– fornecidas como parte dos dados SNMP e
– apresentadas através do painel de controlo como parte dos dados de diagnóstico de rede.

RSTP

O RSTP é um protocolo de rede em conformidade com a norma IEEE. O RSTP assegura que não existem loops nas redes. As vias redundantes são detetadas na rede, desativadas e ativadas quando necessário (falha de uma ligação).

O protocolo é utilizado exatamente com este objetivo na rede.
Uma alteração à topologia após a falha de uma ligação é automaticamente cancelada assim que tenha sido reparada.

5.2 Diâmetro da rede

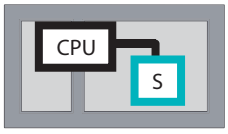
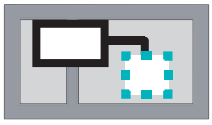
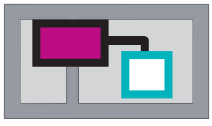
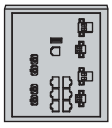
O diâmetro das redes de painel Ethernet RSTP não deve ser superior a 32.

Definição

O diâmetro de uma rede corresponde ao número de switches RSTP na secção mais longa possível sem loops entre quaisquer 2 pontos finais da rede.
Devem ser tidas em conta as seguintes considerações no que respeita à rede de painel Ethernet RSTP:

- Cada painel de controlo contém um ponto final e um switch RSTP interno.
- Uma combinação de painel de controlo e painel de controlo redundante conta apenas como um switch RSTP.
- Os conversores multimédia não são considerados switches RSTP.
- Não é possível incluir ligações CAN na secção mais longa possível.
- Os servidores OPC não são tidos em conta no diâmetro.

Chave

	Processador central no painel de controlo ou no painel repetidor.
	Switch RSTP interno no painel de controlo ou no painel repetidor.
	Painel de controlo ou painel repetidor com processador central e switch RSTP interno.
	Painel de controlo redundante com processador central e switch RSTP interno.
	Painel de controlo ou painel repetidor Ponto de início ou final para determinar o diâmetro da rede nos exemplos.
	Switch Ethernet como switch RSTP externo (em geral, switch Ethernet MM)

2 painéis ligados formam o loop mais pequeno possível. O diâmetro desta rede é igual a 2, dado os switches RSTP internos estarem localizados entre os pontos finais.

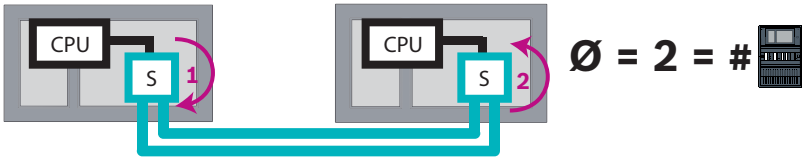


Figura 5.1: Diâmetro da rede de um loop com 2 painéis

Num loop de painéis sem switches RSTP externos, o diâmetro da rede corresponde ao número de painéis instalados.

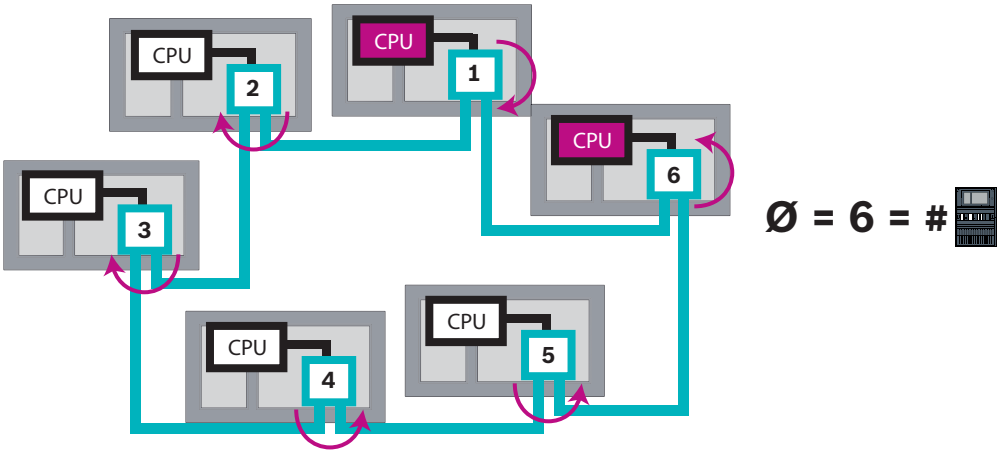


Figura 5.2: Diâmetro da rede de um loop com 6 painéis

Se uma infraestrutura e os subloops estiverem ligados entre si através de switches Ethernet, então estes switches RSTP externos também devem ser tidos em conta.

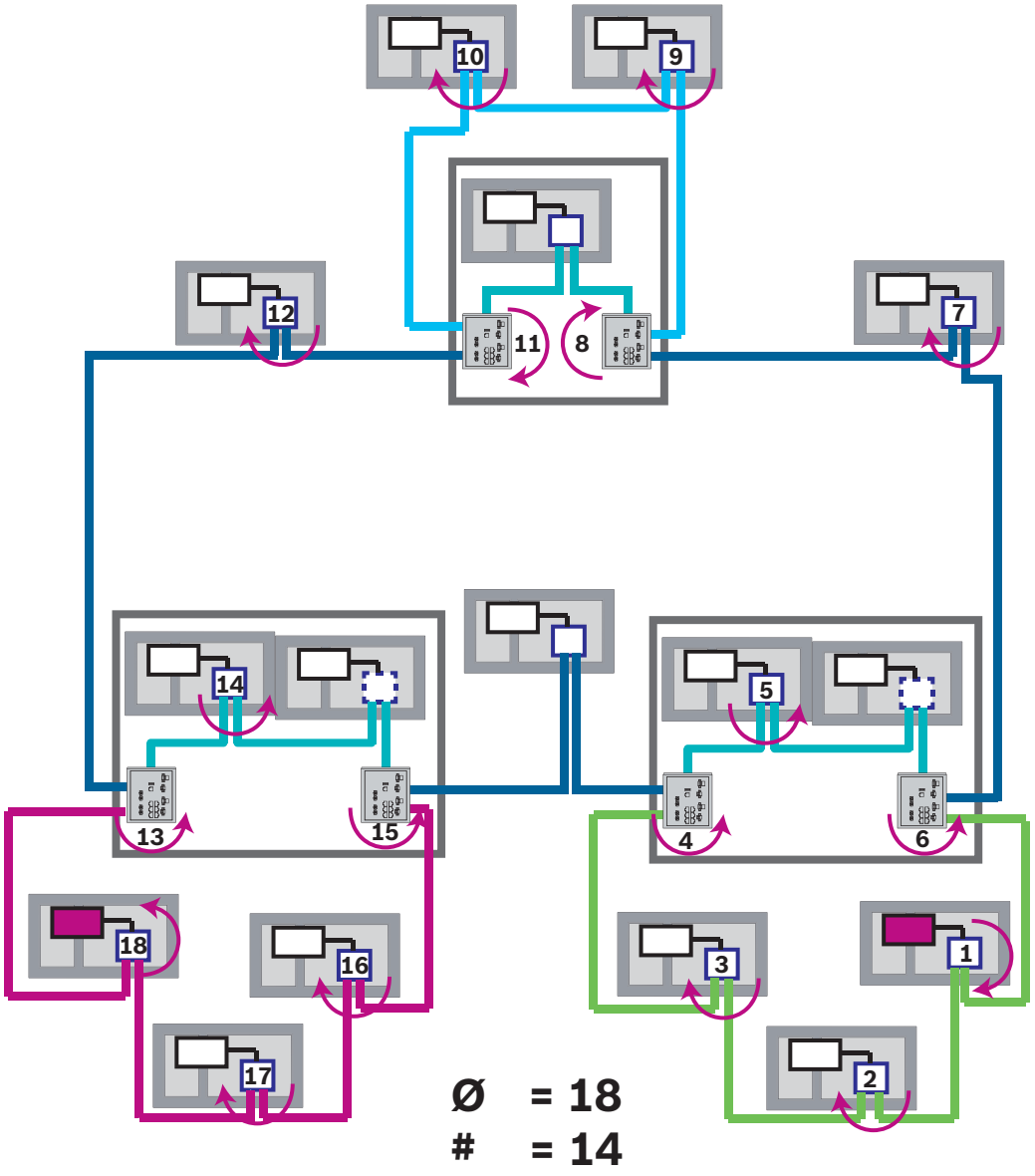


Figura 5.3: Diâmetro de rede de uma infraestrutura com subloops

A figura mostra que para o diâmetro tem de determinar a via mais longa.

5.3 Cabos utilizados

Utilize sempre os cabos de ligação em rede indicados a seguir. A utilização de outros cabos não cumpre as normas de segurança estabelecidas nas diretivas da CE.

– Cabo Ethernet
  Cabo de rede Ethernet, blindado, CAT 5e ou superior.
  Tenha em atenção os raios de curvatura mínimos indicados na especificação do cabo.
– Cabo de fibra ótica
  Modo múltiplo: cabo de rede Ethernet de fibra ótica, I-VH2G 50/125µ duplex ou I-VH2G 62.5/125µ duplex, ficha SC.
  Modo único: cabo de rede Ethernet de fibra ótica, I-VH2E 9/125µ duplex, ficha SC.
  Tenha em atenção os raios de curvatura mínimos indicados na especificação do cabo.

Informação!
Comprimento do cabo TX
Todas as ligações IP devem ser diretas ou realizadas através de conversores multimédia aprovados pela Bosch. O comprimento do cabo TX de nó a nó deve ser inferior a 100 m.

Informação!
VdS 2540
Para cumprir os requisitos de VdS 2540 para caminhos de transmissão de dados, utilize o cabo de fibra ótica para ligações Ethernet. Para ligações dentro de um compartimento, pode utilizar TX Cabos Ethernet.

5.4 Criar ou modificar uma rede Ethernet

Existem vários procedimentos para a criação de uma rede Ethernet de painéis de controlo de alarme de incêndio. Os 2 procedimentos descritos em seguida diferem no tamanho das redes e no número de tarefas de instalação e configuração realizadas em cada um deles.

Regras para a utilização de 4 portas Ethernet
Se o seu painel tiver 4 portas Ethernet, aplique as seguintes regras pela ordem indicada. A Bosch apenas suporta redes criadas de acordo com as regras a seguir.

1. Para a ligação em rede dos painéis, tem de utilizar ETH1 e ETH2. Um switch RSTP externo em ETH1 ou ETH2 só deve ser utilizado para a ligação em rede dos painéis.
2. Para ligar um OPC, um FSM-5000-FSI, um Sistema de alarme por voz, um UGM-2040 tem de utilizar ETH3. Pode ligar um switch RSTP externo que não deve ser utilizado para a ligação em rede dos painéis.
3. Para Remote Services, tem de utilizar ETH4. Se não houver ligação a Remote Services é necessário, então ETH4 pode ser usado para ligar um OPC, um FSM-5000-FSIum Sistema de alarme por voz, ou um UGM-2040.
4. Se não houver uma rede de painéis através de ETH1 e ETH2cada um pode ser utilizado para ligar um OPC, um FSM-5000-FSIum Sistema de alarme por voz, ou um UGM-2040.

Criar uma rede Ethernet (projetos de pequena dimensão)
Este procedimento é adequado para projetos que envolvam apenas um pequeno número de engenheiros a trabalhar em simultâneo na instalação do sistema de alarme de incêndio.

1. Planeie a rede.
2. Crie a rede no FSP-5000-RPS e configure as definições de rede.
3. Imprima as informações da rede de modo a mantê-las em segurança ou guarde-as no portátil.
4. Instale os painéis de controlo e os cabos de rede, e ligue-os a uma rede.
5. Configure as definições de rede para os painéis de controlo individuais diretamente na unidade de controlo de acordo com o documento impresso.
6. Execute o reset de cada um dos painéis de controlo na rede para ativar a configuração da rede.
7. Ligue o seu computador com o software de programação FSP-5000-RPS a um painel de controlo na rede. Carregue esta configuração em todos os outros painéis de controlo da rede através deste painel de controlo. Os painéis redundantes utilizam a configuração do painel principal.
8. Execute um reset de modo a repor as mensagens de erro pendentes. Retifique quaisquer erros.

Configure primeiro as definições de rede nos painéis de controlo. Isto permite-lhe programar os outros painéis de controlo na rede a partir de um painel de controlo.

Criar uma rede Ethernet (projetos de média e grande dimensão)

Este procedimento é adequado para projetos que envolvam uma série de tarefas executadas em simultâneo por diversas equipas. Como muitas tarefas realizadas durante a instalação e a configuração envolvem o reinício do painel de controlo do alarme de incêndio, neste procedimento, a rede só é iniciada numa fase posterior.

1. Planeie a rede.
2. Realize uma configuração da rede sem periféricos com o FSP-5000-RPS.
3. Imprima as informações da rede de modo a mantê-las em segurança ou guarde-as no portátil.
4. Instale os cabos de rede e verifique as secções ou os loops individuais.
5. Instale os painéis e opere-os como painéis autónomos.
6. Instale os periféricos nos painéis.
7. Configure cada painel com o FSP-5000-RPS.
8. Certifique-se de que os painéis individuais estão a funcionar corretamente.
9. Coloque os loops individuais da rede em funcionamento uns a seguir aos outros, de acordo com a topologia.

   Comece pela infraestrutura.
   - Realize uma configuração para a infraestrutura no FSP-5000-RPS. Importe todas as configurações necessárias para os painéis. Configure as definições de rede e imprima-as.
   - Ligue todos os painéis a uma rede.
   - Configure as definições de rede para os painéis de controlo individuais diretamente no painel de controlo de acordo com o documento impresso.
   - Execute o reset de cada um dos painéis de controlo para carregar a configuração de rede.
   - Envie um comando ping para os painéis adjacentes para verificar a rede.
   - Coloque toda a infraestrutura em funcionamento e retifique quaisquer erros.

   Coloque os subloops em funcionamento de acordo com o exemplo da infraestrutura.

Adicionar um painel a uma rede

1. Altere a configuração de rede no FSP-5000-RPS.
2. Imprima as informações da rede de modo a mantê-las em segurança ou guarde-as no portátil.
3. Instale o painel de controlo e os cabos de rede, e ligue-os à rede.
4. Configure as definições de rede para o painel de controlo individual diretamente na unidade de controlo de acordo com o documento impresso.
5. Execute o reset do painel e dos painéis adjacentes para ativar a configuração de rede.

Remover um painel da rede

1. Altere a configuração de rede no FSP-5000-RPS.
2. Imprima as informações da rede de modo a mantê-las em segurança ou guarde-as no portátil.
3. Configure as definições de rede para os painéis de controlo adjacentes diretamente na unidade de controlo de acordo com o documento impresso.
4. Desligue o painel e a alimentação (da rede e bateria) antes de removê-lo da rede.
5. Execute o reset dos painéis adjacentes para ativar a configuração de rede.

6 Rede CAN

Topologia em loop

Numa topologia em loop, o cabo CAN é sempre encaminhado a partir de um terminal CAN1 para um terminal CAN2 [CAN1 ⇒ CAN2]. O comprimento do cabo depende da secção transversal do cabo.

Ligação CAN

A ligação CAN é uma ligação de dois fios (CAN-H e CAN-L). Ligue CAN-H a CAN-H e ligue CAN-L a CAN-L para obter uma ligação de dois fios. Poderá ser necessária uma ligação de três fios (CAN-H, CAN-L e CAN-GND) em casos excecionais; por exemplo, com uma carga EMC elevada ou uma diferença significativa no potencial de ligação à terra. Ligue CAN-H a CAN-H, CAN-L a CAN-L e CAN-GND a CAN-GND para obter uma ligação de três fios. O fio blindado do cabo CAN só está ligado à caixa de metal do painel por um lado.

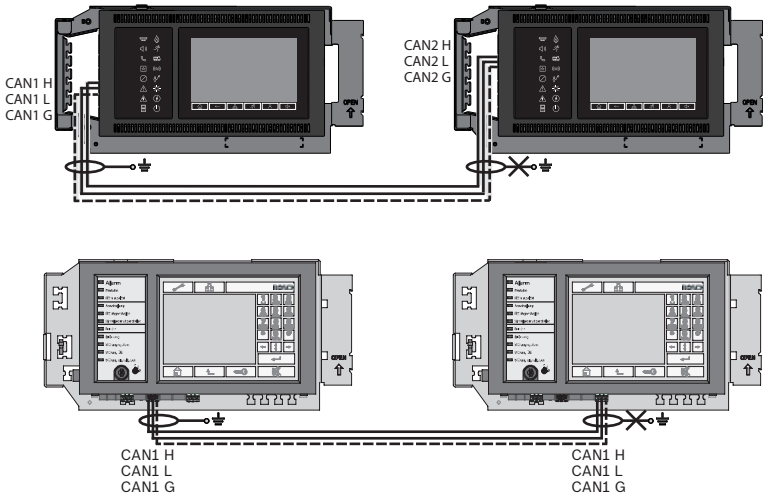


Figura 6.1: Ligação CAN (superior: AVENAR, inferior: FPA)

Comprimento do cabo para ligação em rede

O tamanho máximo do cabo permitido depende da resistência de loop do cabo utilizado e do número de nós de comunicação.

Exemplo: o cabo do detetor de incêndio vermelho J-Y (St) Y 2 x 2 x 0,8 mm permite a ligação de dois nós com uma distância máxima de cerca de 800 m.

Informação!

A distância entre os dois nós na topologia em loop pode ser determinada pela leitura do valor nos dois nós no diagrama.

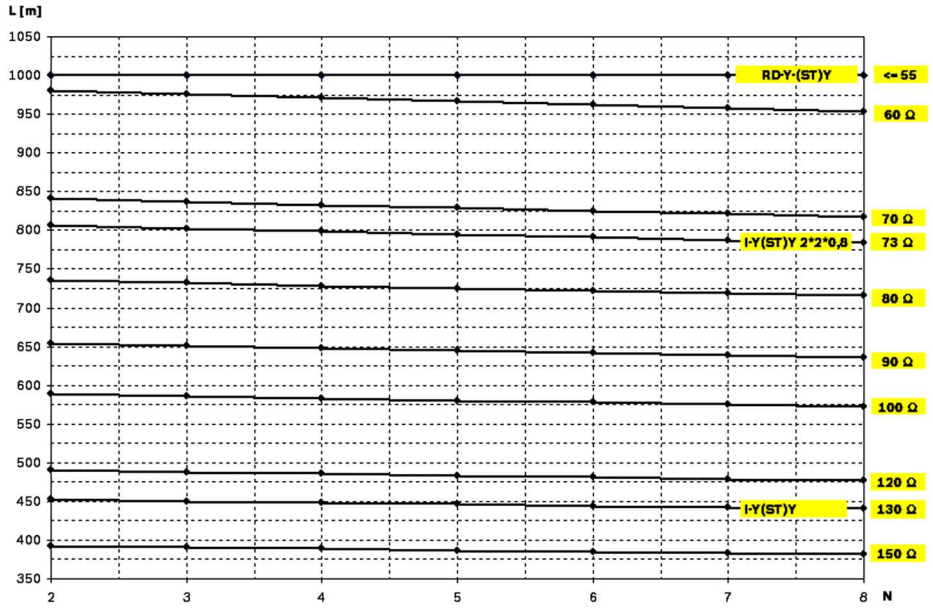


Figura 6.2: Rede CAN: comprimento do cabo que é possível atingir, consoante o número de nós e a resistência do cabo

L = comprimento do cabo em metros

N = número de nós

6.1 Criar ou modificar uma rede CAN

Este procedimento é adequado para projetos que envolvam apenas um pequeno número de engenheiros a trabalhar em simultâneo na instalação do sistema de alarme de incêndio.

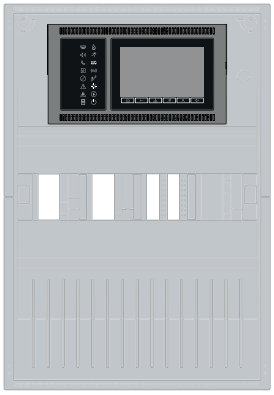
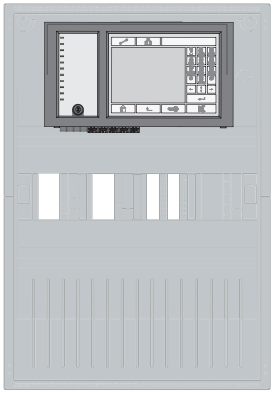
Procedimento para criar uma rede CAN

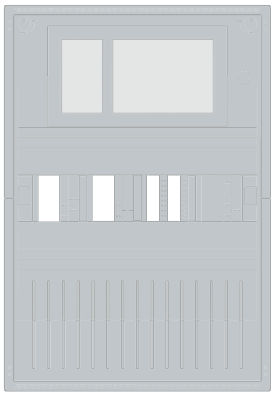
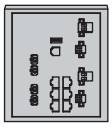
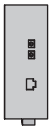
1. Planeie a rede.
2. Crie a rede no FSP-5000-RPS.
3. Imprima as informações da rede de modo a mantê-las em segurança ou guarde-as no portátil.
4. Instale os painéis de controlo e ligue-os com cabos CAN a uma rede.
5. Ligue o seu computador com o software de programação FSP-5000-RPS a um painel de controlo na rede. Carregue esta configuração em todos os outros painéis de controlo da rede através deste painel de controlo. Os painéis redundantes utilizam a configuração do painel principal.
6. Execute um reset de modo a repor as mensagens de erro pendentes. Retifique quaisquer erros.

7 Padrão de ligação em rede Ethernet e CAN

Para criar redes de painel correspondentes às topologias e aos serviços de ligação introduzidos, necessita do padrão de ligação em rede descrito neste documento.

Ícone	Descrição
	TX Cabo Ethernet (cobre), comprimento do cabo TX de nó a nó < 100 m

Ícone	Descrição
	Cabo Ethernet FX (cabo de fibra ótica)
	Cabo Ethernet TX ou FX, comprimento do cabo TX de nó a nó < 100 m
	Cabo CAN
	Caixa Nota: para simplificar a visão geral dos vários padrões de ligação em rede, as figuras deste capítulo mostram sempre uma pequena caixa de painel para simbolizar um painel. Esta pequena caixa **não** fornece em todos os casos apresentados espaço suficiente para montar os switches, os conversores de multimédia e os gateways. Utilize o Safety Systems Designer para garantir que encomenda a quantidade correta e o tamanho correto de caixas para instalar o equipamento.
	AVENAR panel
	FPA

Ícone	Descrição
	AVENAR panel ou FPA
	Switch Ethernet como switch RSTP externo (em geral, switch Ethernet MM)
	Conversor de multimédia
	Gateway de rede segura para Remote Services
	Ligação a OPC servidor, FSM-5000-FSI, Sistema de alarme por voz ou UGM-2040

7.1 Rede de painéis através de Ethernet

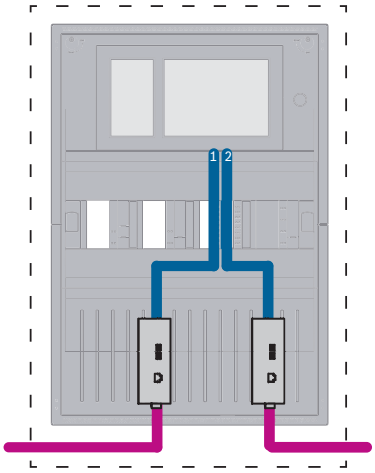


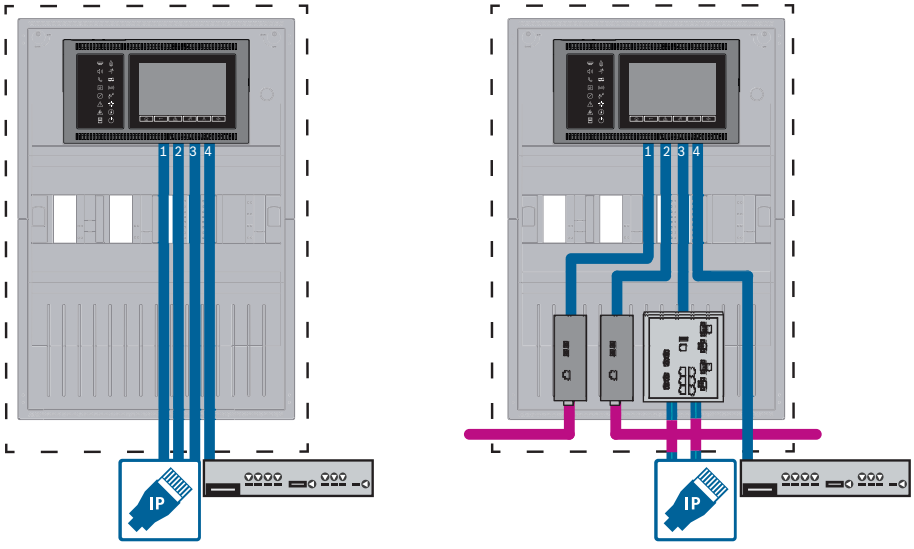
Figura 7.1: Rede de painéis através de Ethernet

Para distâncias superiores a 100 m, é obrigatória a utilização de conversores multimédia. Para distâncias inferiores a 100 m, os conversores multimédia podem não ser necessários.

7.2 Rede de painéis através de CAN

Figura 7.2: Rede de painéis através de CAN

7.3 Ligar os serviços ao painel



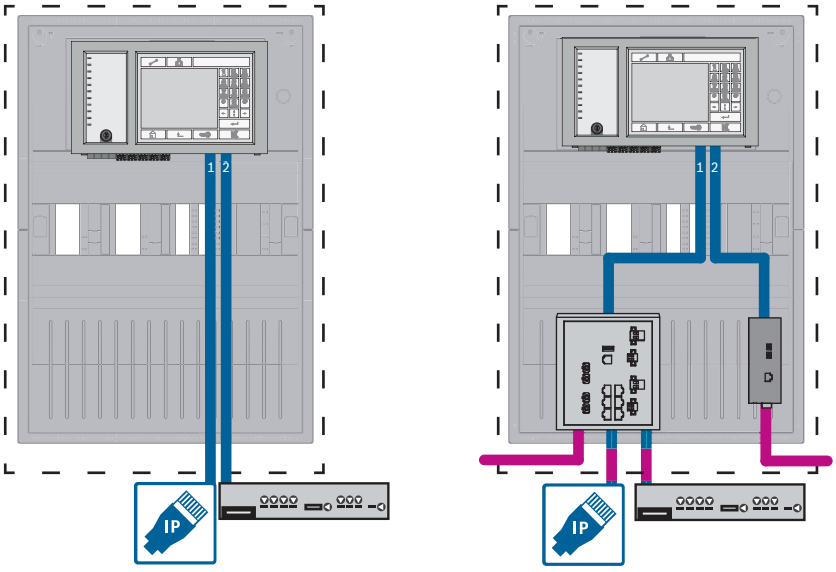


Figura 7.3: Lado esquerdo: sem rede de painéis, Lado direito: com rede de painéis

O switch Ethernet é apenas necessário para mais de dois serviços ligados ao painel.

Para distâncias superiores a 100 m, é obrigatória a utilização de conversores multimédia. Para distâncias inferiores a 100 m, os conversores multimédia podem não ser necessários.

7.4 Rede de painéis através de Ethernet com painéis redundantes

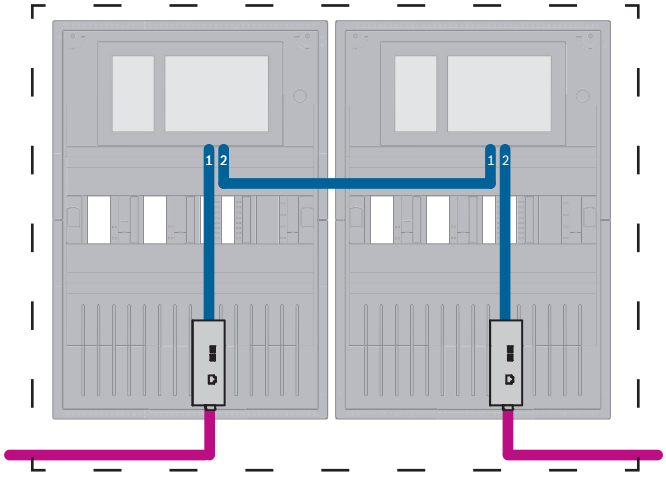


Figura 7.4: Rede de painéis através de Ethernet com painéis redundantes

Para distâncias superiores a 100 m, é obrigatória a utilização de conversores multimédia. Para distâncias inferiores a 100 m, os conversores multimédia podem não ser necessários.

7.5 Rede de painéis através de CAN com painéis redundantes

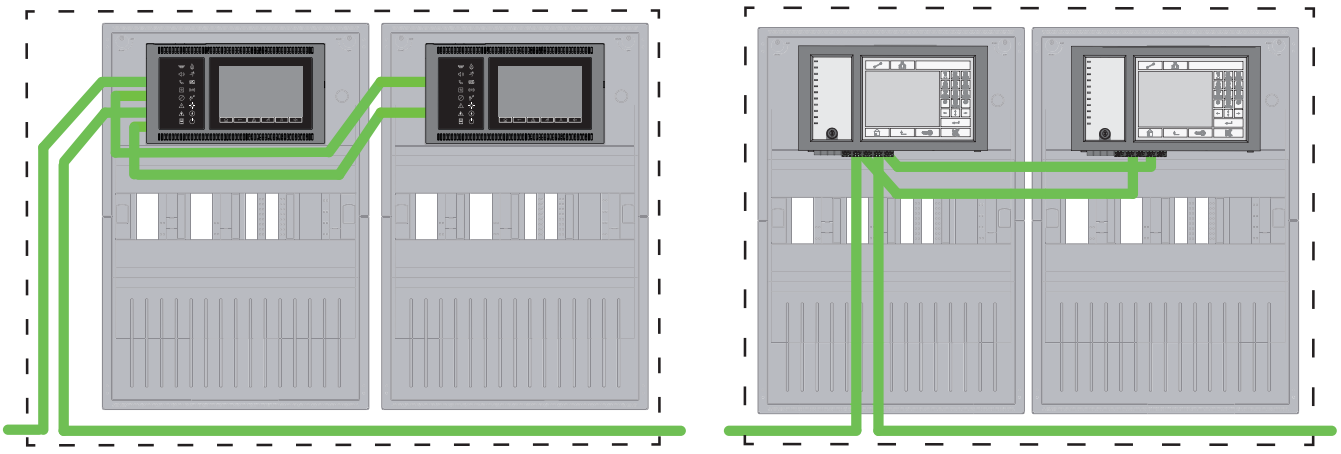


Figura 7.5: Rede de painéis através de CAN com painéis redundantes

7.6 Rede de painéis em dois loops Ethernet

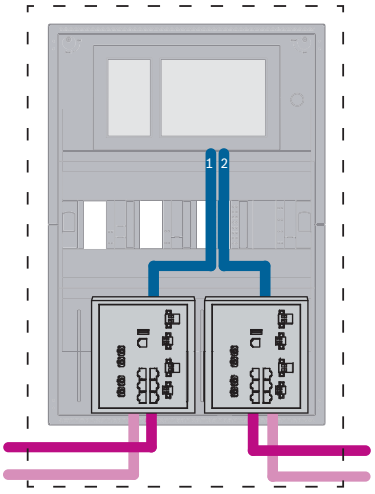


Figura 7.6: Ligar redes Ethernet

7.7 Rede de painéis em dois loops Ethernet com painéis redundantes

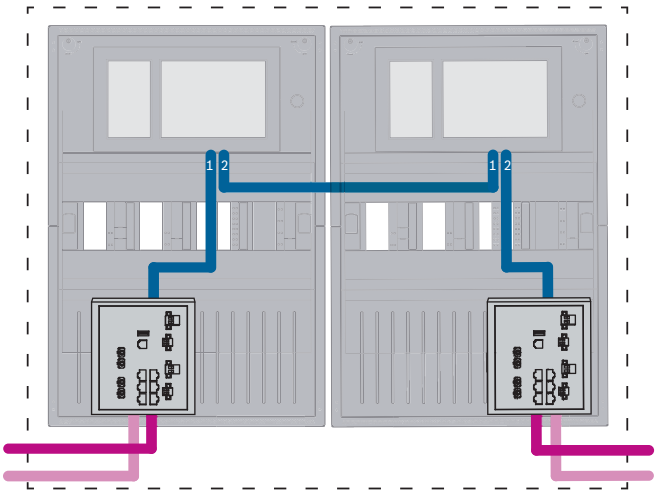


Figura 7.7: Ligar redes Ethernet com painéis redundantes

7.8 Ligar rede Ethernet e CAN com painéis redundantes

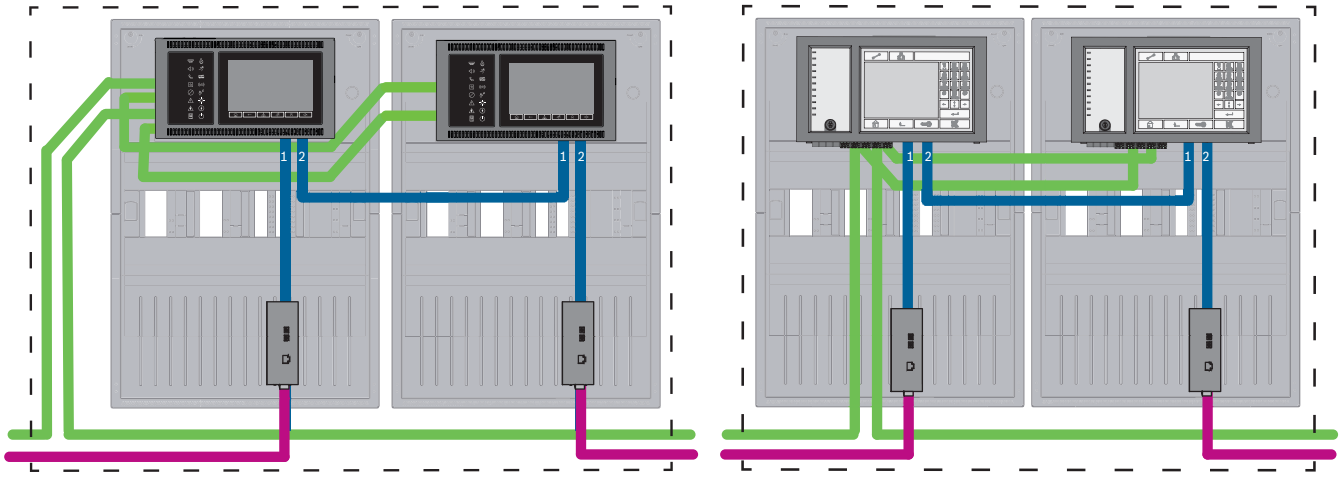


Figura 7.8: Ligar rede Ethernet e CAN com painéis redundantes

Para distâncias superiores a 100 m, é obrigatória a utilização de conversores multimédia. Para distâncias inferiores a 100 m, os conversores multimédia podem não ser necessários.

7.9 Ligar serviços remotos a painéis redundantes

É possível ligar o Secure network gateway a uma FPA redundante ou a uma FPA redundante AVENAR panel. Pelas seguintes razões, não deve ligar o Secure network gateway a um painel redundante por rede AVENAR panel mas sim a um AVENAR panel sem redundância de painel:

- O procedimento é uma solução provisória.
- No caso de uma ligação a um software grafico através de FSM-5000-FSI / OPC a porta ETH3 do controlador do painel redundante deve ser utilizada e configurada.

7.9.1 Painel AVENAR Redundante

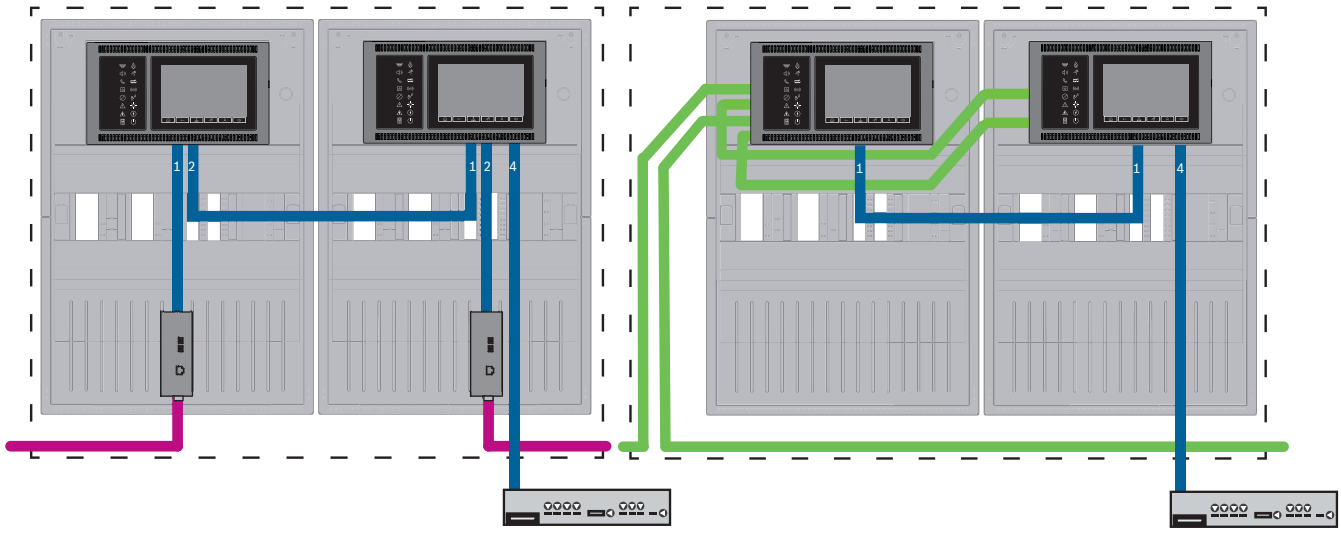


Figura 7.9: Lado esquerdo: na rede Ethernet Lado direito: na rede CAN

Para distâncias superiores a 100 m, é obrigatória a utilização de conversores multimédia. Para distâncias inferiores a 100 m, os conversores multimédia podem não ser necessários.

1. Para ligar o Secure network gateway, ligue-o à porta ETH4 do controlador do painel redundante.

2. Na rede CAN, é necessário um cabo Ethernet da ETH1 para a porta ETH1 do controlador do painel redundante. Configure as ETH1 definições na FSP-5000-RPS **Interface de rede-Ethernet** janela:
   - Para **Tipo de Linha** selecione **Ligação**
   - Um número de linha superior a 0 em **Ligado à linha n.º** faz com que a ligação seja supervisionada.
3. Para ambos, rede CAN ou rede Ethernet, configure as ETH4 definições na FSP-5000-RPS **Interface de rede-Ethernet** janela:
   - Entre em 0 em **Ligado à linha n.º**.
   - Marcar **Utilizar Porta**.

7.9.2 FPA Redundante

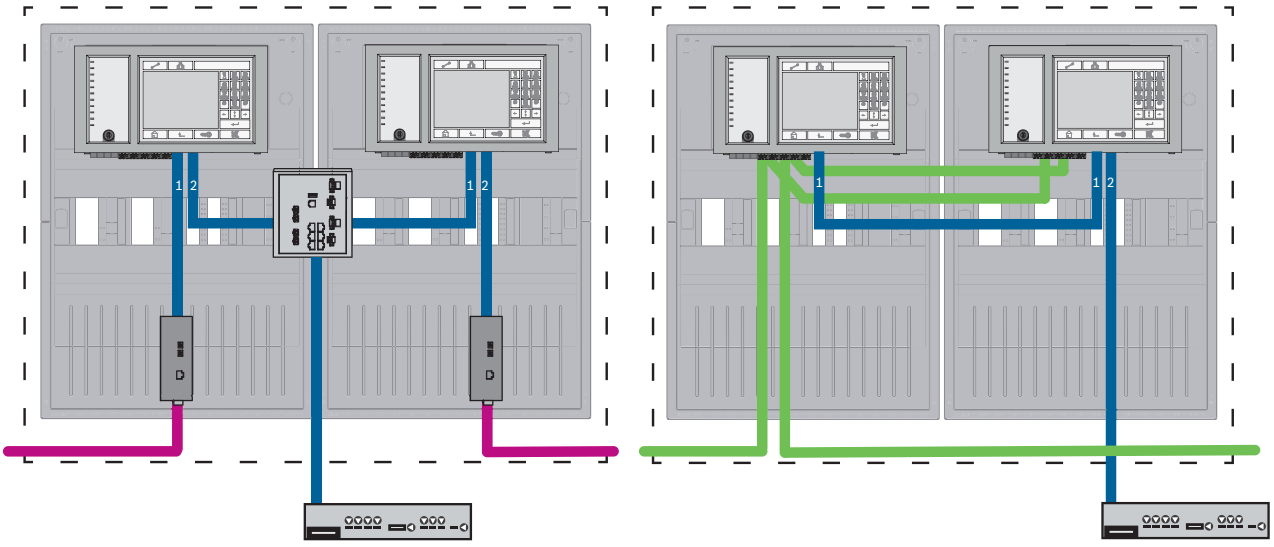


Figura 7.10: Lado esquerdo: na rede Ethernet Lado direito: na rede CAN

Para distâncias superiores a 100 m, é obrigatória a utilização de conversores multimédia. Para distâncias inferiores a 100 m, os conversores multimédia podem não ser necessários.

Procedimento na rede CAN

1. Para ligar o Secure network gateway, ligue-o à porta ETH2 do controlador do painel redundante.
2. Na rede CAN, é necessário um cabo Ethernet da ETH1 para a porta ETH1 do controlador do painel redundante. Configure as ETH1 definições na FSP-5000-RPS **Interface de rede-Ethernet** janela:
   - Para **Tipo de Linha** selecione **Ligação**
   - Um número de linha superior a 0 em **Ligado à linha n.º** faz com que a ligação seja supervisionada.
3. Configure as ETH2 definições na FSP-5000-RPS **Interface de rede-Ethernet** janela:
   - Entre em 0 em **Ligado à linha n.º**.
   - Marcar **Utilizar Porta**.

7.10 Ligue os serviços de segurança e proteção aos painéis redundantes

Deve ligar os serviços de segurança e proteção a um AVENAR panel sem redundância de painel:

– A solução provisória para serviços remotos não é adequada para ligações relevantes para a segurança e proteção a sistemas de alarme por voz (VAS sobre IP) ou a um painel (UGM-2040). Deve ser instalado um EN 54 switch de rede certificado ligado ao controlador do painel principal e ao controlador do painel redundante.

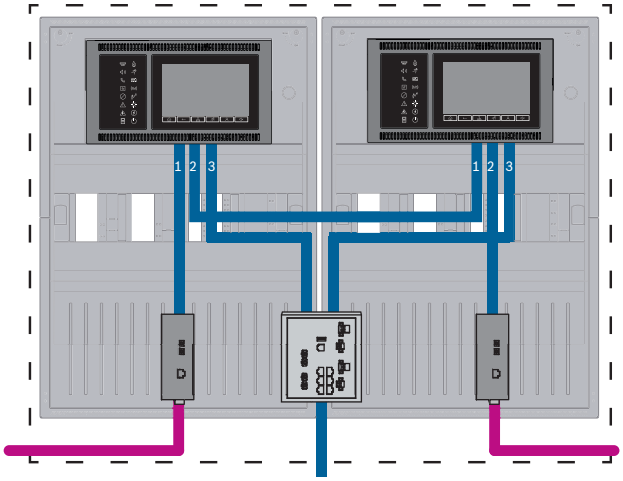


Figura 7.11: VAS e interface para painel AVENAR redundante

8 Remote Services

Os seguintes serviços pertencem a Remote Services:
– Remote Connect
– Remote Alert
– Remote Maintenance

O pré-requisito para Remote Alert e Remote Maintenance é o Remote Connect.

8.1 Remote Connect

O Remote Connect proporciona uma ligação segura e fiável à Internet, o que permite o acesso remoto a um painel através do FSP-5000-RPS. O Remote Connect é a base de todos os Remote Services. Para o Remote Connect, utilize o Gateway de rede segura.
No caso de uma rede de painéis, um painel da rede de painéis tem de ser ligado a um Gateway de rede segura. Esta ligação tem de ser exclusivamente uma ligação Ethernet dedicada.

Informação!
Enquanto que o Remote Connect suporta a ligação a uma rede de painéis através de Ethernet ou CAN, as funcionalidades Remote Alert e Remote Maintenance só são suportadas quando uma ligação em rede Ethernet entre os painéis é fornecida e configurada para utilização do serviço.

O Remote Connect tem de estar ativado na configuração FSP-5000-RPS deste painel.
A topologia seguinte mostra painéis de controlo ligados através da Ethernet em que um Gateway de rede segura está ligado à rede através de um switch Ethernet (em geral, MM).

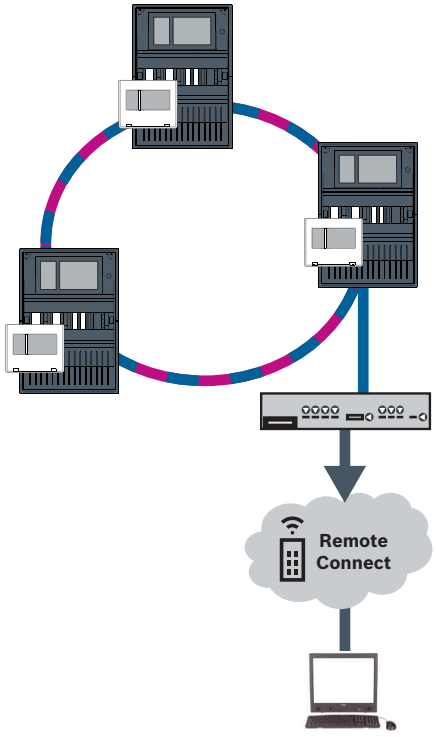


Figura 8.1: Remote Connect num loop Ethernet

Informação!
Para ligar painéis via FX, utilize conversores multimédia aprovados pela Bosch.

Para impedir o envio de tráfego multicast relevante de EN 54-2 ao router, utilize o switch Ethernet (em geral, MM, BPA-ESWEX-RSR20) aprovado com a versão de painel 2.8. Ativar IGMP snooping do switch Ethernet, veja a secção correspondente no capítulo Instalação do Manual de Rede.

Informação!
O router de Internet (ou a rede da empresa que fornece o acesso à Internet) e o Gateway de rede segura têm de fornecer sub-redes separadas. Os painéis da rede de painéis não podem ser inseridos na sub-rede do router da Internet. Além disso, a sobreposição das sub-redes não é possível.
No caso de uma sobreposição de sub-redes, tem de separar as sub-redes alterando os endereços IP no lado da rede do painel.
Também tem de propagar as alterações no Gateway de rede segura. Para tal, inicie a interface da Web através do browser da Web:
- Endereço: https://192.168.1.254
- Nome de utilizador: bosch
- Palavra-passe: ipti83

Pode alterar o endereço IP em **Configuração** -> **Rede (LAN)**. Tenha em atenção que o endereço do **Gateway predefinido:** na configuração do painel de controlo tem de corresponder ao endereço IP do Gateway de rede segura.

Informação!
De acordo com as diretrizes do DIBt, o reset remoto não é permitido através dos Remote Services para restaurar a prontidão operacional dos sistemas de controlo de portas com assistência de abertura motorizada.

A topologia seguinte mostra uma rede CAN em que o Gateway de rede segura está ligado à rede através de uma porta Ethernet.

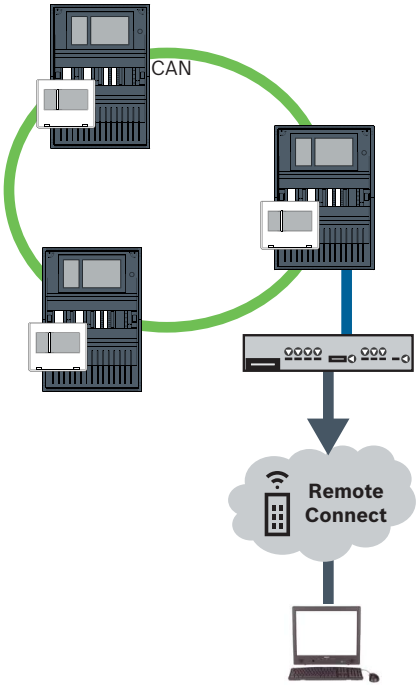


Figura 8.2: Remote Connect num loop CAN

8.2 Remote Alert

O Remote Alert permite que um painel envie informações de estado relevantes ao Remote Portal.
Os dados transferidas são analisados com o Remote Alert. Em caso de um evento inesperado, o utilizador será informado por SMS e/ou e-mail sobre os alertas recebidos.
O Remote Alert também está disponível para Private Secure Network.

8.3 Remote Maintenance

O Remote Maintenance permite monitorizar remotamente determinados parâmetros de diversos itens de segurança ligados a um painel de incêndio. Pode realizar testes de passagem através do Remote Portal.

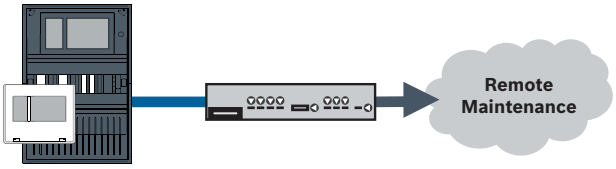


Figura 8.3: Remote Maintenance

Informação!
As ligações Ethernet utilizadas apenas para transferir dados do Remote Maintenance poderão ser efetuadas através de cabos Ethernet ou de fibra ótica. Tenha em atenção os comprimentos máximos permitidos para os cabos.

Informação!
Para ligar painéis via FX, utilize conversores multimédia aprovados pela Bosch.

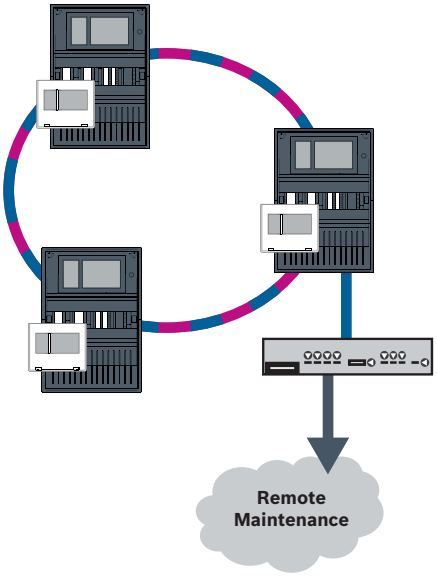


Figura 8.4: Remote Maintenance

Quando utiliza o Remote Maintenance com redes Ethernet, é necessário ligar um painel na rede ao router para fins de transferência de dados. Todos os dados recolhidos são transferidos a partir da rede através desta ligação.

Remote Maintenance para Remote Portal

O Remote Maintenance recolhe dados de módulos funcionais e dispositivos LSN relevantes, e envio-os ao Remote Portal onde são analisados e visualizados para atividades de manutenção.

Remote Maintenance para Rede Segura Privada

O Remote Maintenance também pode ser configurado para a Private Secure Network: os dados recolhidos serão enviados para um sistema de servidor de gestão central (CMS).

Atenção!
O Remote Services necessita de uma ligação IP segura. Necessita do Remote Services da Bosch ou da ligação à Private Secure Network.
Com a Private Secure Network é fornecida uma rede IP baseada em DSL com acesso sem fios opcional no lado do painel (EffiLink). O Remote Services para a Private Secure Network só está disponível na Alemanha mediante celebração de um contrato de serviço com a Bosch BT-IE.

Informação!
Para ligar painéis via FX, utilize conversores multimédia aprovados pela Bosch.

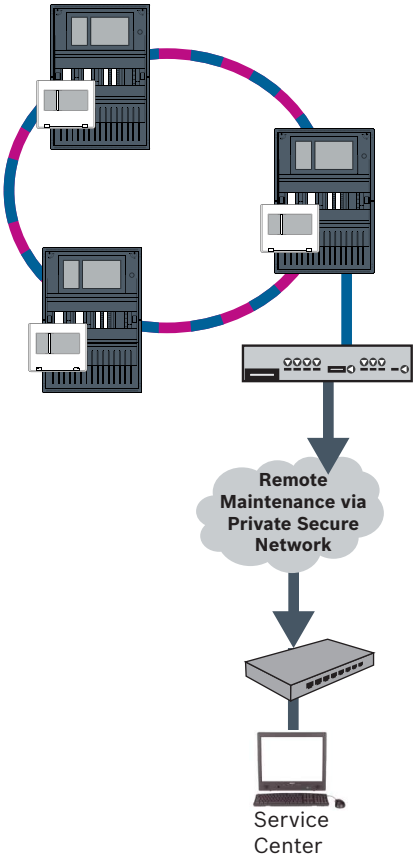


Figura 8.5: Remote Maintenance para Rede Segura Privada

Para o Remote Maintenance, tem de introduzir o endereço IP do servidor e a porta do servidor de sistema do Remote Maintenance no software de programação FSP-5000-RPS.
Atribua um ID de rede de painéis exclusivo à rede.

O switch para ligação do CMS tem de ser programado em separado.
Programe o endereço IP e as definições de redundância do switch; consulte *Definições do interruptor, página 51*. Como o switch é instalado nas proximidades imediatas (sem espaço intermédio), a fonte de alimentação não tem de ser projetada de forma redundante e as saídas de falha não são consequentemente utilizadas.
Certifique-se de que as definições de RSTP nos painéis de controlo, no FSP-5000-RPS e no switch Ethernet são idênticas.

8.4 Remote Portal

Requisitos

Informação!
Para evitar reconfigurações ou ajustes ao utilizar o Remote Services, certifique-se de que os seguintes requisitos foram cumpridos:
- painel com firmware 2.19.7 ou superior, todos os painéis ligados através de Ethernet, interfaces de Ethernet ativadas e definições de Ethernet padrão
- Remote Connect ativado na configuração do painel FSP-5000-RPS
- Gateway de rede segura para Remote Services disponível
- computador com FSP-5000-RPS 4.8 ou superior instalado e acesso à Internet

Informação!
Evite atualizar o Gateway de rede segura durante a ligação.
As atualizações do Gateway de rede segura são executadas regularmente durante a madrugada. Assim, especifique o fuso horário em **Sistema** -> **Definições gerais** -> **Fuso horário**.

Instruções
Para utilizar o Remote Services, tem de ser utilizador de uma conta do Remote Portal.

Passo 1: Criar uma conta do Remote Portal
Podem existir vários utilizadores numa conta do Remote Portal. Cada conta do Remote Portal tem um Remote ID exclusivo, destinado a representar uma empresa. Se não conseguir utilizar uma conta do Remote Portal existente, tem de criar uma:

1. Em https://remote.boschsecurity.com -> **Inscrever-se**, introduza o seu nome, a sua empresa e o seu endereço de e-mail, e crie uma palavra-passe. Leia os termos e condições, e selecione **Concordo com os termos e condições**. Leia também a declaração de privacidade e selecione **Concordo coma declaração de privacidade**.
2. Clique em **Registar**.
   O Remote Portal enviará de imediato um e-mail com um endereço para a ligação de ativação.
3. Para ativar a conta, clique na ligação de ativação. No Remote Portal, clique no nome de utilizador e selecione **Definições da conta**. É apresentado o Remote ID. Posteriormente, irá necessitar deste Remote ID no painel de controlo.

Para fornecer a cada um dos seus técnicos uma conta individual, pode criar vários utilizadores para o mesmo Remote ID:
Inicie sessão no Remote Portal.

- Selecione **Utilizadores** -> **Novo técnico**. Em seguida, introduza os dados necessários e confirme com **Gravar**.

Passo 2: Ligar o Gateway de rede segura
Para estabelecer o Remote Services, utilize um Gateway de rede segura.

1. Ligue a porta WAN do Gateway de rede segura ao router de Internet ou à rede empresarial que fornece o acesso à Internet.
2. No router de Internet ou na rede empresarial, verifique a disponibilidade dos seguintes protocolos e portas para o Gateway de rede segura (necessário para ligação ao Remote Services).

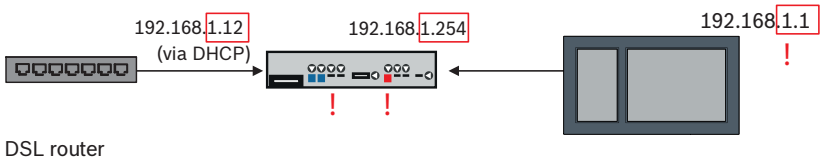
Protocolo	Porta predefinida	Descrição
HTTP	80 e 8080	para registo do Remote Connect e Remote Maintenance
VPN IPsec	UDP 500 e UDP 4500	para Remote Connect

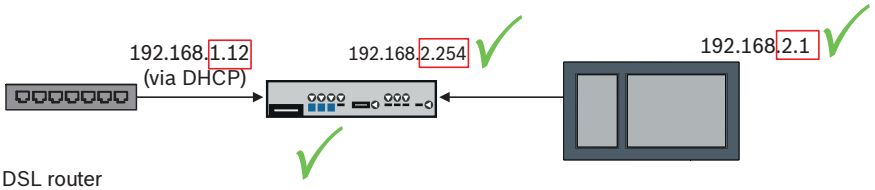
3. Ligue a porta LAN1 do Gateway de rede segura à porta Ethernet designada do painel de controlo utilizando o cabo de rede CAT5 RJ45 fornecido. Observe as possíveis topologias.
4. Ligue o Gateway de rede a uma alimentação de rede de 100 V - 230 V com a fonte de alimentação fornecida.

O LED WAN acende-se (azul) quando a ligação à Internet for estabelecida. O LED VPN acende-se (azul) pouco depois, o que indica que foi estabelecida uma ligação VPN ao Remote Portal. Cada painel ou rede de painéis ligados tem um System ID exclusivo.

Separar sub-redes (LED VPN desligado)

A ligação do Gateway de rede segura para Remote Services falha caso existam sub-redes sobrepostas (LED VPN desligado). O exemplo seguinte mostra um Gateway de rede segura e um painel de controlo no mesmo intervalo de endereços que o router DSL.





Um Gateway de rede segura deteta sub-redes sobrepostas de forma precisa: o LED Alarm pisca continuamente.

A separação das sub-redes é efetuada mediante a alteração do terceiro octeto do endereço IP. Os endereços IP são alterados no lado da rede do painel. Depois de alterar o endereço IP, tem de propagar as alterações no Gateway de rede segura. Para tal, inicie a interface da Web através do browser da Web:

- Endereço: https://192.168.1.254
- Nome de utilizador: bosch
- Palavra-passe: ipti83

Pode alterar o endereço IP em **Configuração** -> **Rede (LAN)**. Tenha em atenção que o endereço do **Gateway predefinido:** na configuração do painel de controlo tem de corresponder ao endereço IP do Gateway de rede segura.

Passo 3: Estabelecer uma ligação remota

1. No painel, utilize a opção de definições de Ethernet.

2. Reinicie o painel.
3. Para a autenticação, selecione **Configuração** -> **Serviços de rede** -> **Alterar data/hora**, introduza a data atual e confirme as suas definições.
4. Selecione **Configuração** -> **Serviços de rede** -> **Remote Services** e introduza o Remote ID.

Pode verificar o estado da ligação remota: selecione **Diagnostics** -> **Network Services** -> **Remote Services** no painel de controlo.

Passo 4: Atribuir uma licença no Remote Portal

Para ativar a utilização do Remote Services, tem de atribuir uma licença no Remote Portal. Uma licença é automaticamente fornecida à sua conta após a primeira ligação efetuada com êxito.

Informação!

Uma licença que já tenha sido atribuída não pode ser reatribuída nem suspensa.

1. Em https://remote.boschsecurity.com -> **Iniciar sessão**, introduza o seu endereço de e-mail e a sua palavra-passe.
2. Selecione **Sistemas**.
3. Selecione o sistema.
4. Em **Serviços**, clique no botão **Adicionar serviço** junto ao serviço.
5. Por predefinição, a licença é renovada automaticamente (**Definições de serviço**, opção **Com renovação automática**).
6. Clique em **Gravar** para confirmar as definições.

Depois de atribuir a licença, pode utilizar o serviço correspondente. Um cadeado verde indica uma licença atribuída.

Passo 5: Reencomendar a licença

1. Encomende licenças de um ano para os Sistemas de alarme de incêndio da Bosch. Cada rede necessita de licenças próprias. A
   Bosch enviará um e-mail para o endereço fornecido. O e-mail inclui números de registo da licença exclusivos consoante a quantidade de licenças encomendadas, bem como instruções e uma ligação para o Remote Portal.
2. Em https://remote.boschsecurity.com -> **Iniciar sessão**, introduza o seu endereço de e-mail e a sua palavra-passe.
3. Selecione **Licenças**.
4. Clique no botão **+**.
5. Siga as instruções apresentadas na janela **Adicionar licenças** e confirme com **Gravar**.
6. A lista de licenças é atualizada.

9 Ligação de segurança inteligente

Este capítulo especifica a solução técnica para uma interface Ethernet segura entre Bosch painéis de incêndio e Bosch sistemas de alarme por voz.

Smart Safety Link é a interface mais fiável e segura para combinar uma deteção de incêndio e um sistema de alarme por voz (VAS). Smart Safety Link oferece uma flexibilidade excecional e opções para a expansibilidade.

A comunicação de dados bidirecional estabelece uma ligação supervisionada entre o painel de deteção de incêndios e o VAS. Tanto o painel de incêndio como o VAS indica uma mensagem de falha quando a ligação é interrompida. No caso de uma ligação interrompida, o utilizador pode iniciar a evacuação do edifício completo manualmente, utilizando uma estação de chamada do VAS. Uma interrupção da interface não leva a uma evacuação automática do

edifício. Quando a interface é restabelecida, o painel de incêndio re-sincroniza automaticamente o estado de alarme atual com o VAS. Em caso de incêndio, o painel de incêndio pode iniciar automaticamente os anúncios de voz utilizando VAS disparos que são ativados por regras que são configuradas em FSP-5000-RPS. O painel de incêndio gera uma mensagem de supervisão quando um evento de evacuação é iniciado a partir do VAS. Uma avaria no VAS irá gerar uma mensagem de falha na interface do utilizador do painel de incêndio.
Através da interface gráfica do utilizador de AVENAR panel o operador tem a possibilidade de silenciar os anúncios do painel de incêndio. O operador pode solicitar uma descrição geral do estado de todos os disparos virtuais. Cada disparo virtual pode ser marcado com uma etiqueta inequívoca contendo a localização e o tipo de mensagem. Uma cor claramente distinta está a refletir a condição de cada disparo virtual. Um operador com L2 os direitos do utilizador podem começar e parar o anúncio de voz no disparo virtual selecionado manualmente.
PAVIRO ou Praesideo pode ser ligado a FPA e AVENAR panel.
Devido à sua topologia em rede PRAESENSA requer uma interface com comunicação de dados encriptados. Só usar AVENAR panel a funcionar na versão de firmware do controlador do painel 4.x para se ligar com PRAESENSA.
Smart Safety Link na Ethernet foi introduzido na versão de firmware do controlador do painel 2.11 e FSP-5000-RPS versão 4.3.

Aviso!
Riscos de segurança na ligação por Ethernet
Não ligue o PRAESENSA a FPA-5000/FPA-1200 utilizando Smart Safety Link devido a riscos de segurança na ligação por Ethernet

Informação!
Sistema de alarme por voz ligado ao painel AVENAR
Cada painel de incêndio que está fisicamente ligado a um sistema de alarme por voz através de Smart Safety Link precisa de uma licença premium.

Informação!
Sistema de alarme por voz ligado à FPA
Cada painel de incêndio que está fisicamente ligado a um sistema de alarme por voz através de Smart Safety Link e a execução de firmware versão 3.x não requer uma chave de licença para alarme por voz.

9.1 Uma interface VAS direta

O painel de incêndio e o sistema de alarme por voz podem ser ligados por um único cabo Ethernet TX.

Informação!
VdS 2540
O sistema de alarme por voz deve estar nivelado com o painel de incêndio numa única sala. Caso contrário, os requisitos de VdS 2540 para vias de transmissão de dados não são cumpridos.

9.1.1 Praesideo e PAVIRO

AVENAR panel e FPA pode ser diretamente ligado à porta Ethernet dedicada ao controlador do sistema de Praesideo (PRS-NCO-3) ou PAVIRO (PVA-4CR12).

Pode utilize a interface "Open Interface" para um único painel ou para uma rede de painéis.

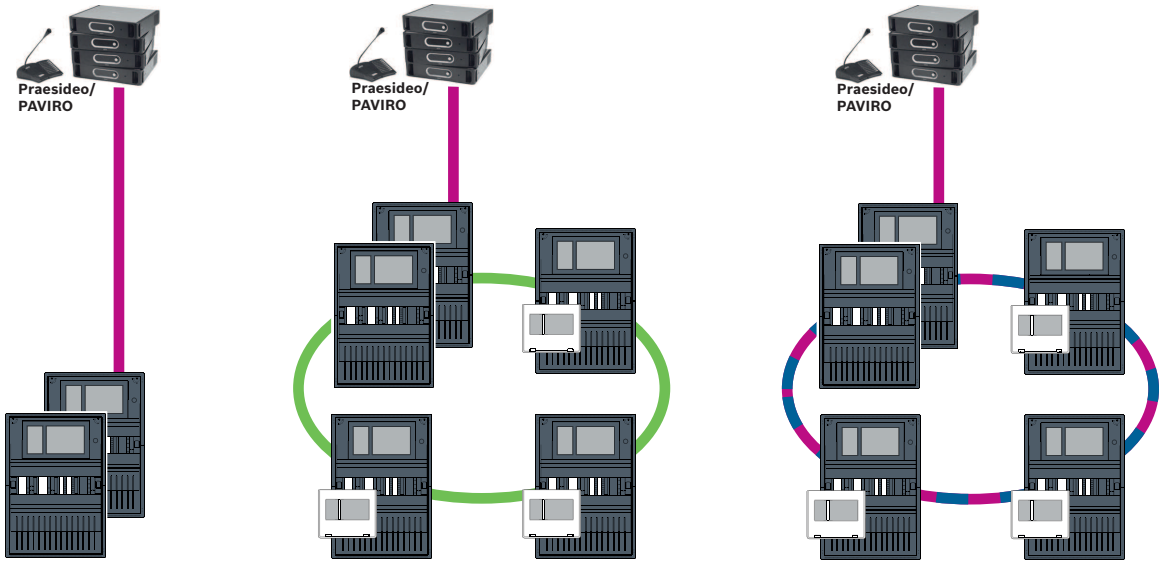


Figura 9.1: Uma interface direta ao Praesideo|PAVIRO

Informação!
Se um painel de controlo MPC-xxxx-B for utilizado para a ligação direta de um sistema Praesideo/PAVIRO, é necessário um cabo de ligação cruzado, uma vez que nem Praesideo/PAVIRO nem MPC-xxxx-B suportam MDI(X) automático.

9.1.2 PRAESENSA

PRAESENSA é um sistema de alarme por voz em rede que utiliza uma rede IP para áudio e controlo.
Ligue sempre AVENAR panel através de um PRA-ES8P2S Switch Ethernet, 8xPoE, 2xSFP para PRAESENSA.

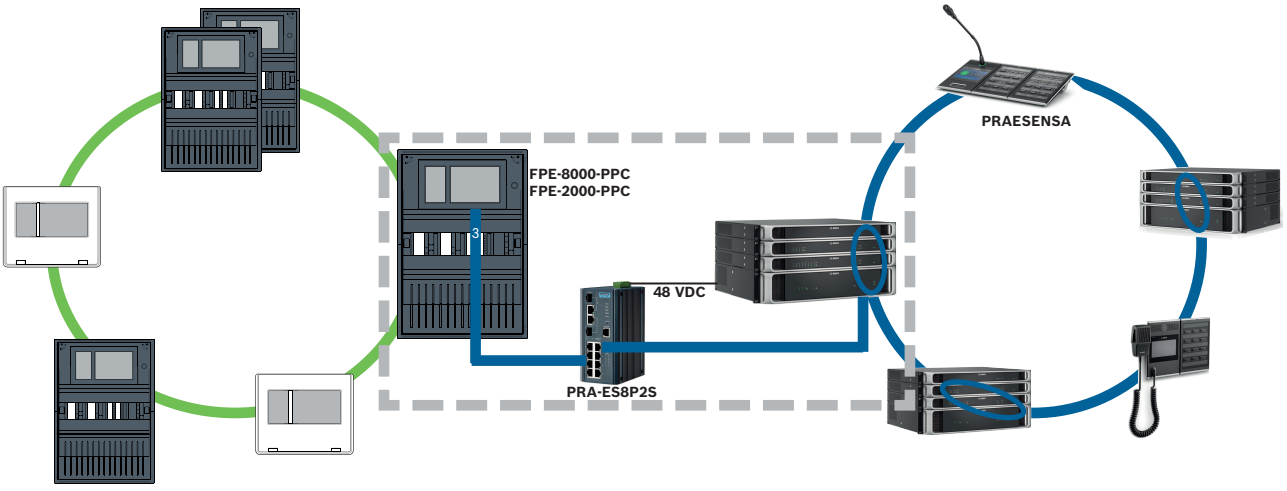


Figura 9.2: Painel PRAESENSA a AVENAR

Atenção!
Riscos de segurança Ethernet
Não utilizar Smart Safety Link para ligar PRAESENSA para FPA-5000/FPA-1200. Só utilizar AVENAR panel e AVENAR keypad 8000 na rede completa. Para ligar PRAESENSA para FPA-5000/FPA-1200 utilize contactos de relé conforme especificado em TI2363/2021. Caso contrário, ocorrem riscos de segurança Ethernet.

Informação!

Painel PRAESENSA a AVENAR

- Utilize PRA-ES8P2S exclusivamente para Smart Safety Link. Para além da PRA-SCL o controlador do sistema não liga outros PRAESENSA equipamentos às portas Ethernet do switch Ethernet, 8xPoE, 2xSFP. Não utilize o switch Ethernet, 8xPoE, 2xSFP para ligação a um Software Gráfico, painel Hierárquico, Gateway de Rede Segura para Serviços Remotos, etc.
- Utilize um painel contendo apenas um controlador de painel para se ligar com PRAESENSA utilizando Smart Safety Link. Smart Safety Link para PRAESENSA ainda não é compatível com a redundância do controlador de painel. Os painéis da rede que não estão diretamente ligados a PRAESENSA podem conter redundância de controladores de painel.
- Utlize a topologia de barramento CAN para a rede de painéis. Não utilize uma rede de painéis Ethernet.
- Todos AVENAR panel e todos AVENAR keypad 8000 na rede devem funcionar com o firmware do painel 4.x.

1. Monte o PRA-ES8P2S switch Ethernet no PRAESENSA bastidor. Instale PRA-SCL de nivelar para AVENAR panelnuma única divisão. Não monte o PRA-ES8P2S switch Ethernet no armário AVENAR panel.
2. PRAESENSA deve fornecer a energia para PRA-ES8P2S.
3. Configure o PRA-ES8P2S switch Ethernet:
   – permitir apenas a comunicação unicast entre FPE-8000-PPC e PRAESENSA controlador
   – bloquear todas as comunicações multicast
   – desativar RSTP
4. Verifique o modo de PRAESENSA deve funcionar em DHCP modo. Zeroconf não é suportado quando se utiliza o modo Smart Safety Link.
5. Ligue o PRAESENSA Controlador por um único cabo Ethernet (RSTP desativado).
6. Para a Smart Safety Link configuração de AVENAR panel, selecione **SVA Encriptado sobre IP** em FSP-5000-RPS.

9.2 Múltiplas interfaces VAS diretas

Numa rede CAN, cada painel de incêndio pode ser ligado a um sistema de alarme por voz. Aplique a ligação de interface direta conforme especificado em *Uma interface VAS direta, página 45*.

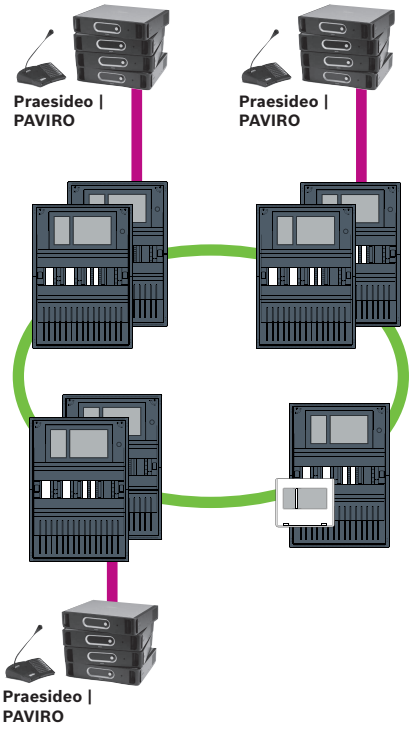


Figura 9.3: Múltiplas interfaces VAS

Para cada nó, para o qual deseja desativar a rede de painéis sobre IP, execute o seguinte procedimento em FSP-5000-RPS:

1. Selecione o nó para desativar a rede de painéis.
2. Selecione **Utilizar Definições da Ethernet**.
3. Deselecione **Ligação em rede do painel através de IP**.
4. Clique em **Aplicar**.

9.3 VAS integrado na rede de painéis Ethernet

Se Praesideo e PAVIRO estão integrados em redes de painéis, depois o sistema de alarme por voz tem um caminho de transmissão redundante. O caminho de transmissão redundante permite que o painel de alarme de incêndio e o sistema de alarme por voz sejam instalados em salas/divisões separadas.
Atualmente não é possível integrar PRAESENSA para uma rede de painéis Ethernet.

Informação!
VdS 2540
O sistema de alarme por voz deve estar nivelado com o painel de incêndio numa única sala. Caso contrário, os requisitos de VdS 2540 para vias de transmissão de dados não são cumpridos.

Informação!
VdS 2540
Para cumprir os requisitos de VdS 2540 para caminhos de transmissão de dados, utilize o cabo de fibra ótica para ligações Ethernet. Para ligações dentro de um compartimento, pode utilizar TX Cabos Ethernet.

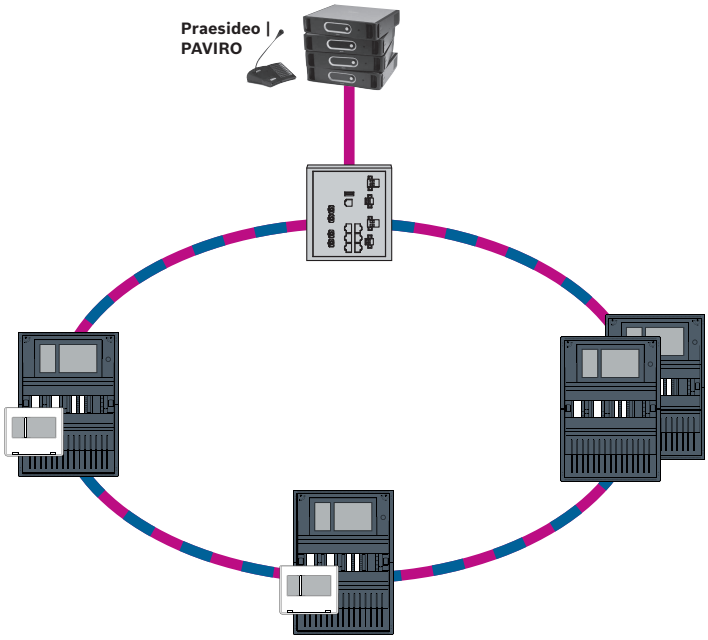


Figura 9.4: VAS integrado na rede de painéis Ethernet

Para impedir o envio de tráfego multicast relevante de EN 54-2 ao router, utilize o switch Ethernet (em geral, MM, BPA-ESWEX-RSR20) aprovado com a versão de painel 2.8. Ativar IGMP snooping do switch Ethernet, veja a secção correspondente no capítulo Instalação do Manual de Rede.

O sistema de alarme de incêndio deve fornecer a energia para o switch Ethernet.

10 Instalação

Lista de verificação

Antes de iniciar a instalação da rede, reveja todos os pontos enumerados abaixo.

- Ethernet e CAN
  - Os comprimentos de linha requeridos dos cabos Ethernet TX, Ethernet FX, CAN TX e CAN FX são inferiores ao comprimento máximo.
  - Todos os periféricos e respetiva cablagem nos painéis individuais estão planeados.
- Projeto da rede
  - Todos os endereços IP e as definições de rede para os painéis individuais e os componentes de rede adicionais estão planeados e disponíveis.
  - Está disponível uma descrição geral dos componentes adicionais a instalar, como switches Ethernets e conversores multimédia, e da respetiva cablagem com painéis adjacentes.
  - Está disponível uma descrição geral da topologia da rede a instalar.
  - Todas as definições de redundância da rede foram planeadas e estão disponíveis.

10.1 Definições no conversor multimédia

Só são precisos alguns passos para utilizar o conversor multimédia:

- Defina os switches DIP.
- Ligue o conversor multimédia aos cabos de rede FX e aos cabo de rede CAT5e.
- Forneça energia ao conversor multimédia através do módulo de controlador da bateria BCM interno.

Informação!
Os conversores multimédia só podem receber energia através do terminal de alimentação 1. O LED de erro existente no conversor multimédia fica, como tal, continuamente iluminado. No entanto, isso não afeta a funcionalidade do dispositivo.

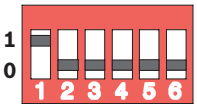
Informação!
Utilize sempre os seguintes cabos na ligação em rede:
Cabo Ethernet
Cabo de rede Ethernet, blindado, CAT5e ou superior.
Tenha em atenção os raios de curvatura mínimos indicados na especificação do cabo.
Cabo de fibra ótica
Modo múltiplo: cabo de rede Ethernet de fibra ótica, I-VH2G 50/125µ duplex ou I-VH2G 62.5/125µ duplex, ficha SC.
Modo único: cabo de rede Ethernet de fibra ótica, I-VH2E 9/125µ duplex
Tenha em atenção os raios de curvatura mínimos indicados na especificação do cabo.

Informação!
Consulte os manuais de instalação dos kits de montagem para obter informações sobre como instalar um conversor multimédia na caixa de um painel: FPM 5000 KMC(F.01U.266.845)FPM-5000-KES(F.01U.266.844)

Informação!
A secção de transmissão máxima para os conversores multimédia de modo múltiplo através de FX é de 2000 m.
A secção de transmissão máxima para os conversores multimédia de modo único através de FX é de 40 Km.

Configure o conversor multimédia com os switches DIP, tal como apresentado na figura seguinte.

Informação!
Altere apenas as definições dos interruptores DIP em conversores multimédia quando estes não estiverem a receber alimentação.



Número de switch DIP	Definição
1	Link Fault Pass-Through ativado
2	Ethernet: modo automático
3	Ethernet: 100 MBit
4	Ethernet: totalmente duplex
5	Cabo de fibra ótica: totalmente duplex
6	Ligação indisponível: desligado

10.2 Instalar switch Ethernet

Aviso!
Luz laser
Não olhe diretamente para o feixe tanto a olho nu como através de instrumentos de visualização de qualquer tipo (por exemplo, lupa ou microscópio). O incumprimento deste aviso representa um perigo para os olhos a uma distância inferior a 100 mm. A luz emerge nos terminais visuais ou na extremidade dos cabos de fibra ótica ligados a estes. Díodo laser CLASSE 2M, comprimento de onda 650 nm, potência < 2 mW, de acordo com a IEC 60825-1.

Informação!
Consulte: Manual de instalação para o kit de montagem do switch Ethernet FPM-5000-KES (F.01U.260.523).

10.3 Definições do interruptor

Para conseguir utilizar os interruptores na rede, tem de os programar.
Ligue o seu portátil à rede e utilize o software HiDiscovery fornecido pelo fabricante para efetuar a programação inicial dos interruptores. Com este software, procure os interruptores existentes na rede. Faça duplo clique no interruptor para o selecionar e atribua-lhe um endereço IP.
Após a programação inicial do endereço IP, pode utilizar um browser da Web para ir para interface de utilizador de configuração do interruptor.

Informação!
Consulte o manual do utilizador do fabricante para obter uma descrição exata da instalação e da configuração dos interruptores. Dados de acesso:
Utilizador: admin
Palavra-passe: private

Utilize um browser para ir para a interface do utilizador de configuração dos interruptores.
Tem de efetuar as seguintes definições no interruptor:
- *Atribua um endereço IP, página 51*,
- *Programe as definições de redundância, página 52*.

Existem ainda as seguintes definições opcionais:
- *Programar o relé de falha, página 52*,
- *Programar a monitorização da ligação, página 53*,
- *Ativação do IGMP snooping, página 54*.

10.3.1 Atribua um endereço IP

Informação!
Sugestão útil:
Na parte do dispositivo para endereços IP, utilize números superiores a 200 (xxx.xxx.xxx.200) para switches, se a sua configuração de rede o permitir. Isso irá separar claramente o identificador anfitrião de um endereço IP.
Exemplo:
O switch 192.168.1.201 é atribuído ao painel com o endereço IP 192.168.1.1.

Informação!
Consulte os seguintes documentos do fabricante para obter uma descrição exata da instalação e da configuração dos switches:
Manual de operação da instalação
Manual de referência da interface baseada na Web

Utilize um browser para aceder à interface do utilizador de configuração do switch.
No menu **Definições básicas -> Rede**, defina os seguintes valores consoante a topologia escolhida:
- Modo: local
- Endereço IP: o endereço IP necessário; por exemplo, 192.168.1.201
- Ecrã de rede: o ecrã de rede necessário: por exemplo, 255.255.255.0
- Gateway: o gateway necessário; por exemplo, 192.168.1.254 ou 0.0.0.0 se não for necessário nenhum gateway.

Clique em **Gravar**.

Informação!
As definições nos itens de menu individuais da configuração do switch são aplicadas depois de clicar em **Gravar**.
As definições só são guardadas de forma permanente, ou seja, de modo a serem mantidas mesmo que o dispositivo seja reiniciado, se, em **Definições básicas -> Carregar/Gravar** no campo **Gravar**, tiver selecionado o item **No dispositivo** e clicado no botão **Guardar**.

10.3.2 Programe as definições de redundância

Como as redes de painéis FPA utilizam o RSTP como protocolo de redundância, é necessário ativar e programar o protocolo na interface do utilizador da configuração:
No menu **Redundancy -> Spanning Tree -> Global** (Redundância -> Árvore Geradora -> Global), defina os seguintes valores:
- Function: On (Função: Ativada)
- Protocol version: RSTP (Versão do protocolo: RSTP)
- Configuração do protocolo: Utilize as mesmas definições dos painéis de controlo.

Clique em **Write** (Gravar).

Informação!
As definições nos itens de menu individuais da configuração dos interruptores ficam válidas depois de clicar em **Write** (Gravar).
As definições só são guardadas de forma permanente, ou seja, de modo a serem mantidas mesmo que o dispositivo seja reiniciado, se, em **Basic Settings -> Load/Save** (Definições básicas -> Carregar/guardar) no campo **Save** (Guardar), tiver selecionado o item **On the device** (No dispositivo) e clicado no botão **Save** (Guardar).

10.3.3 Programar o relé de falha

Informação!
O relé de falha só tem de ser programado para aplicações em que, pelo menos, um dos seguintes requisitos esteja preenchido:
Existe uma ligação entre dois switches. Isso é possível, por exemplo, no caso de uma infraestrutura com subloops.
A alimentação do switch é concebida de forma redundante.

Informação!
Consulte os seguintes documentos do fabricante para obter uma descrição exata da instalação e da configuração dos switches:
Manual do utilizador da instalação
Manual de referência da interface baseada na Web

Utilize um browser para ir para a interface do utilizador de configuração do switch.
Em **Diagnosis -> Signal Contact** (Diagnóstico -> Contacto de sinal) no separador **Signal Contact 1** (Contacto de sinal 1), defina o **Signal Contact Mode** (Modo de contacto de sinal) como **Device Status** (Estado do dispositivo).
Em **Diagnosis -> Device Status** (Diagnóstico -> Estado do dispositivo) no campo **Monitoring** (Monitorização), defina os seguintes valores:
– **Power Supply 1**: **Monitor** (Fonte de alimentação 1: Monitor)
– **Connection Error**: **Monitor** (Erro de ligação: Monitor)
Todas as outras definições devem ser configuradas como **Ignore** (Ignorar).

Informação!
As definições em **Device Status** (Estado do dispositivo) também se aplicam ao LED de falha do switch.

Clique em **Write** (Gravar).

Informação!
As definições nos itens de menu individuais da configuração dos switches ficam válidas depois de clicar em **Write** (Gravar).
As definições só são guardadas de forma permanente, ou seja, de modo a serem mantidas mesmo que o dispositivo seja reiniciado, se, em **Basic Settings -> Load/Save** (Definições básicas -> Transferir dados/guardar) no campo **Save** (Guardar), tiver selecionado o item **On the device** (No dispositivo) e clicado no botão **Save** (Guardar).

10.3.4 Programar a monitorização da ligação

Informação!
A definição de monitorização da ligação só é necessária se estiver a utilizar o relé de falha do interruptor.

Se pretender utilizar o relé de falha para monitorizar as ligações do interruptor, é necessário especificar, na configuração do interruptor, as portas do interruptor que devem ser monitorizadas.
Ative a caixa de verificação **Forward Connection Error** (Reencaminhar erro de ligação) individualmente para cada porta no menu **Basic Settings -> Port Configuration** (Definições básicas -> Configuração de portas).
Só são monitorizadas ligações para as quais a caixa de verificação **Forward Connection Errors** (Reencaminhar erro de ligação) tenha sido ativada.
Clique em **Write** (Gravar).

Informação!
As definições nos itens de menu individuais da configuração dos interruptores ficam válidas depois de clicar em **Write** (Gravar).
As definições só são guardadas de forma permanente, ou seja, de modo a serem mantidas mesmo que o dispositivo seja reiniciado, se, em **Basic Settings -> Load/Save** (Definições básicas -> Carregar/guardar) no campo **Save** (Guardar), tiver selecionado o item **On the device** (No dispositivo) e clicado no botão **Save** (Guardar).

10.3.5 Prioridade de QoS, apenas para UGM-2040

Se utilizar os switch para a comunicação entre as redes de painéis de incêndio e o UGM-2040, então a prioridade de QoS deve ser definida nos switch do UGM.
No menu QoS/Priorität -> Global, altere as definições do campo de lista pendente em Trusted Mode para trustIpDscp.
Clique em **Write** (Gravar).

Informação!
As definições nos itens de menu individuais da configuração dos interruptores ficam válidas depois de clicar em **Write** (Gravar).
As definições só são guardadas de forma permanente, ou seja, de modo a serem mantidas mesmo que o dispositivo seja reiniciado, se, em **Definições básicas -> Carregar/Gravar** no campo **Gravar**, tiver selecionado o item **No dispositivo** e clicado no botão **Guardar**.

10.3.6 Ativação do IGMP snooping

Para evitar o envio de EN 54-2 tráfego multicast relevante para outros sistemas ligados ao Ethernet Switch (Sistema de alarme por voz integrado na rede de painéis Ethernet, Remote Connect) ativar IGMP snooping.
Na página de configuração do IGMP no Ethernet Switch, selecione as seguintes opções:

1. Ative o funcionamento do **IGMP** snooping.
2. Ative o **IGMP Querier** (Pesquisador IGMP).
3. Configure o intervalo de transmissão em que o RSR20 envia pacotes de consulta IGMP (por exemplo, 4 segundos).
4. Configure o tempo em que os membros do grupo multicast devem responder às consultas IGMP (por exemplo, 3 segundos).
5. Selecione **Discard** (Rejeitar) em pacotes com endereços multicast desconhecidos.
6. Selecione **Send to Query and registered Ports** (Enviar para portas registadas e de consulta) em pacotes com endereços multicast conhecidos.
7. Ative o IGMP apenas em portas em que outros sistemas ligados ao switch estejam ligados. Desative a opção **Static Query Port** (Porta de consulta estática) em todas as portas.

10.4 Rede CAN

Ligação em rede e interfaces
O painel de controlo tem

- duas interfaces CAN (CAN1/CAN2) para ligação em rede (topologia loop ou de ramal)
- duas entradas de sinal (IN1/IN2)
- duas interfaces Ethernet
- interface USB

Dependendo do tipo do painel de controlo:

- mais duas interfaces Ethernet
- interface RS232

Tenha em atenção que o comprimento máximo do cabo para ligação da interface USB é de 3 m e para a ligação da interface RS232 é de 2 m.

Endereçamento e definições da rede

Dependendo do tipo do painel de controlo:

– O endereço de nó físico do painel definido no firmware do painel quando liga o painel pela primeira vez.
– RSN em interruptores rotativos mecânicos na parte posterior do painel

Para mostrar o endereço de nó físico, se estiver no painel de controlo:

▸ Selecione **Configuração** -> **Serviços de rede** -> **Ethernet** -> **Utilizar definições de Ethernet** -> **Definições de IP** -> **Predefinições**

Para alterar o endereço de nó físico guardado no painel de controlo:

▸ Mostre as predefinições e altere o último número do **endereço IP**.

Para alterar um RSN mecânico:

▸ Nos interruptores rotativos mecânicos existentes na parte posterior do painel, defina o RSN e anote-o na sinalização abaixo dos mesmos.

Configuração da topologia

Os interruptores DIP para a configuração de diferentes topologias estão localizados na parte posterior.

▸ Assinale a definição selecionada na sinalização existente junto aos interruptores DIP.

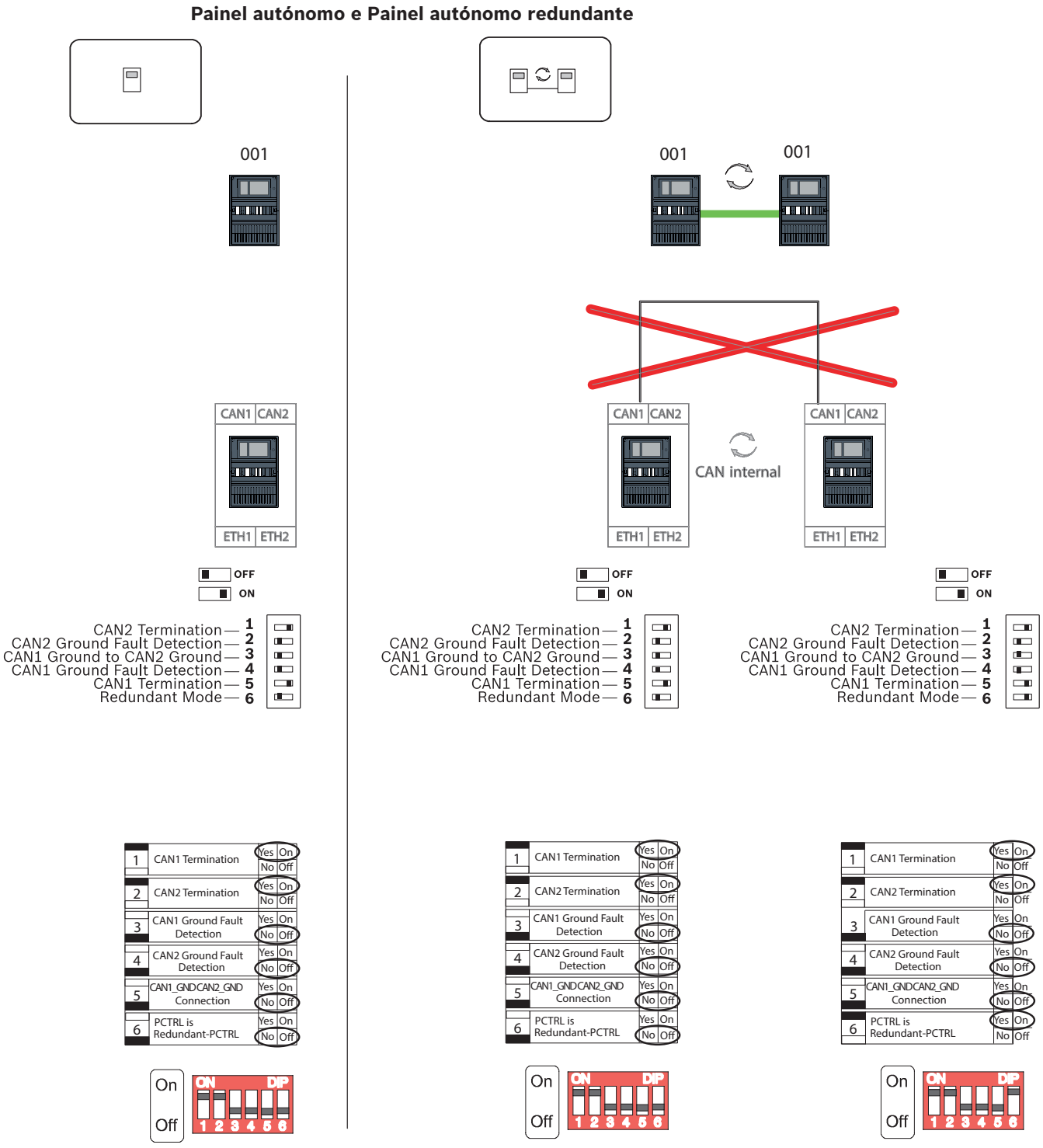


Figura 10.1: Definições do interruptor DIP para o painel autónomo (superior: AVENAR, inferior: FPA, esquerdo: normal, direito: redundante)

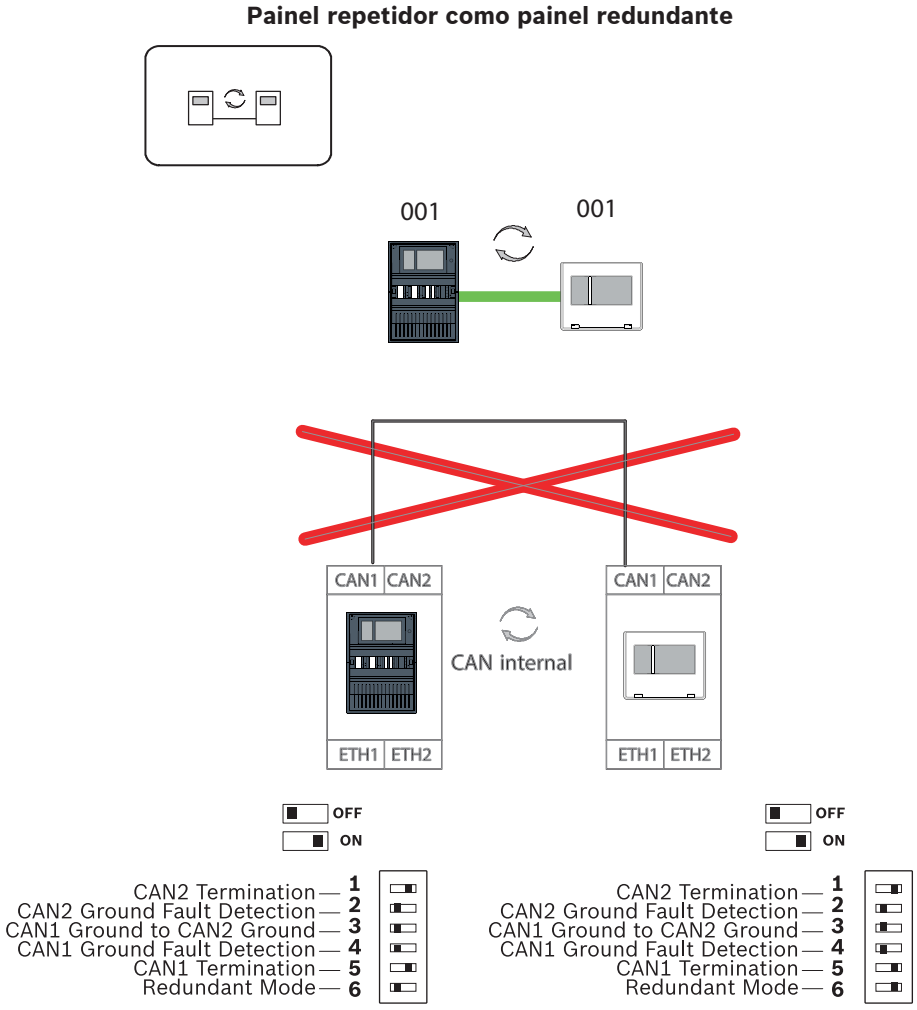


Figura 10.2: Definições do interruptor DIP para painel repetidor como painel redundante (apenas AVENAR)

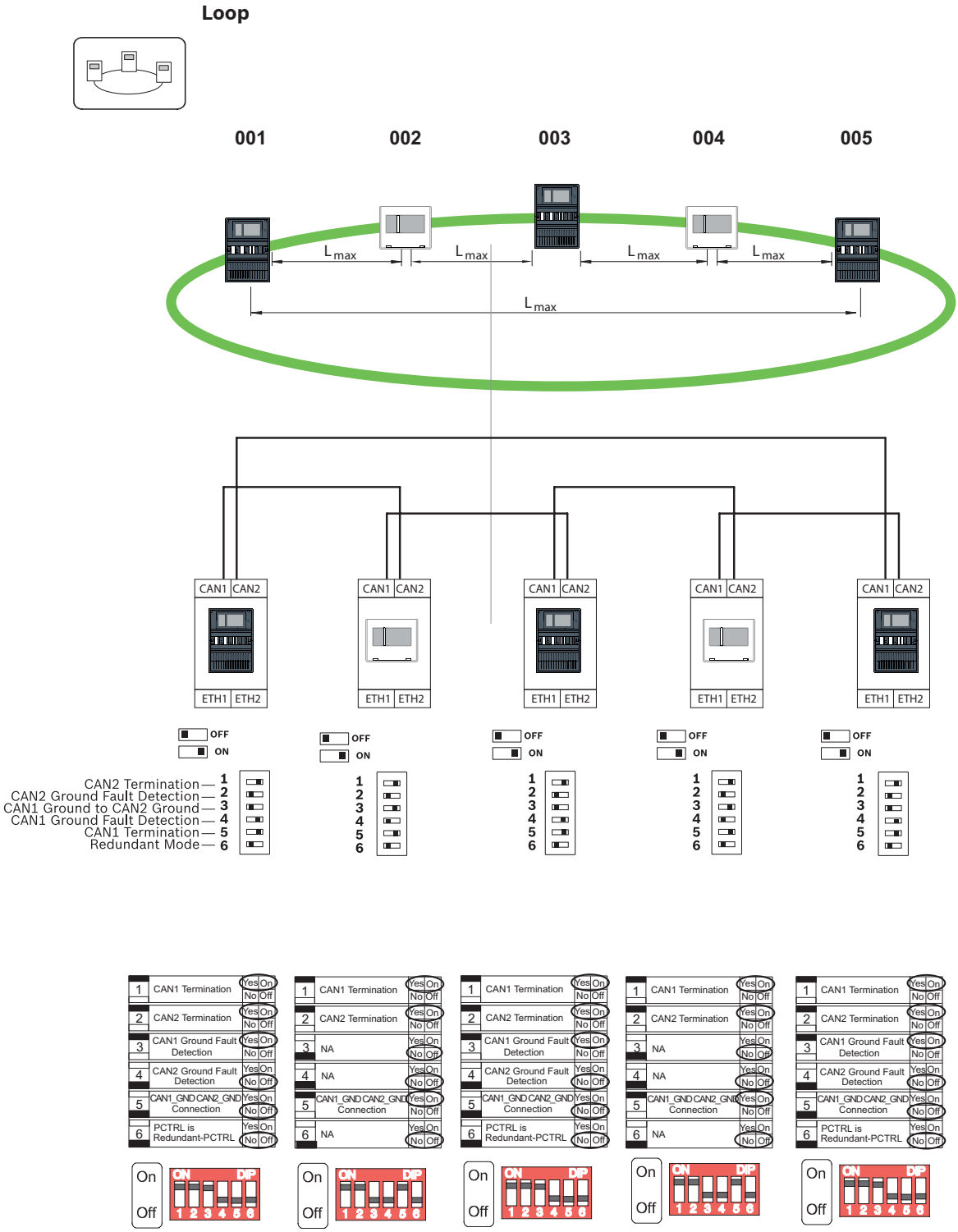


Figura 10.3: Definições do interruptor DIP para loop (superior: AVENAR, inferior: FPA)

Loop com painéis redundantes

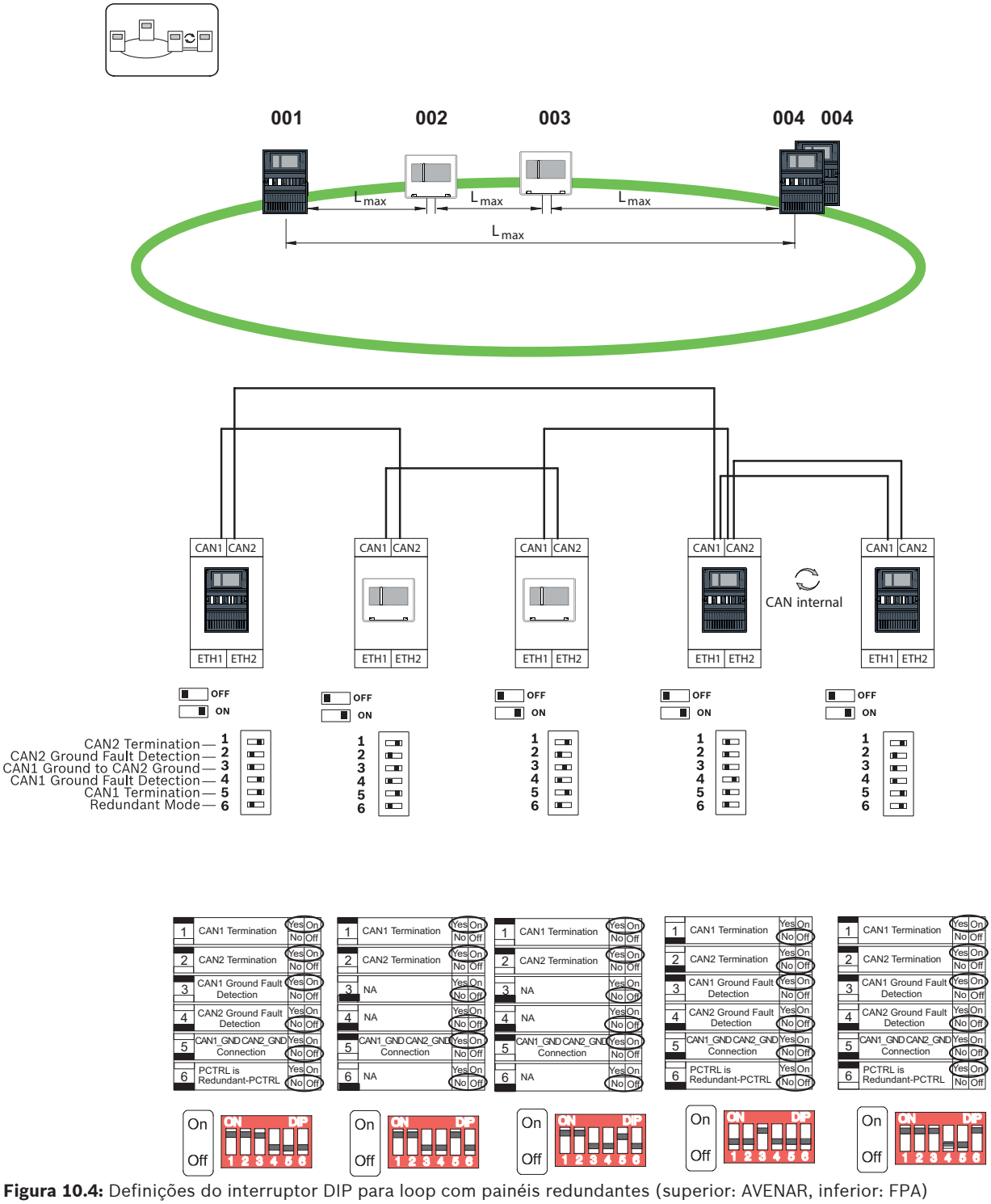


Figura 10.4: Definições do interruptor DIP para loop com painéis redundantes (superior: AVENAR, inferior: FPA)

Loop com painel repetidor como painel redundante

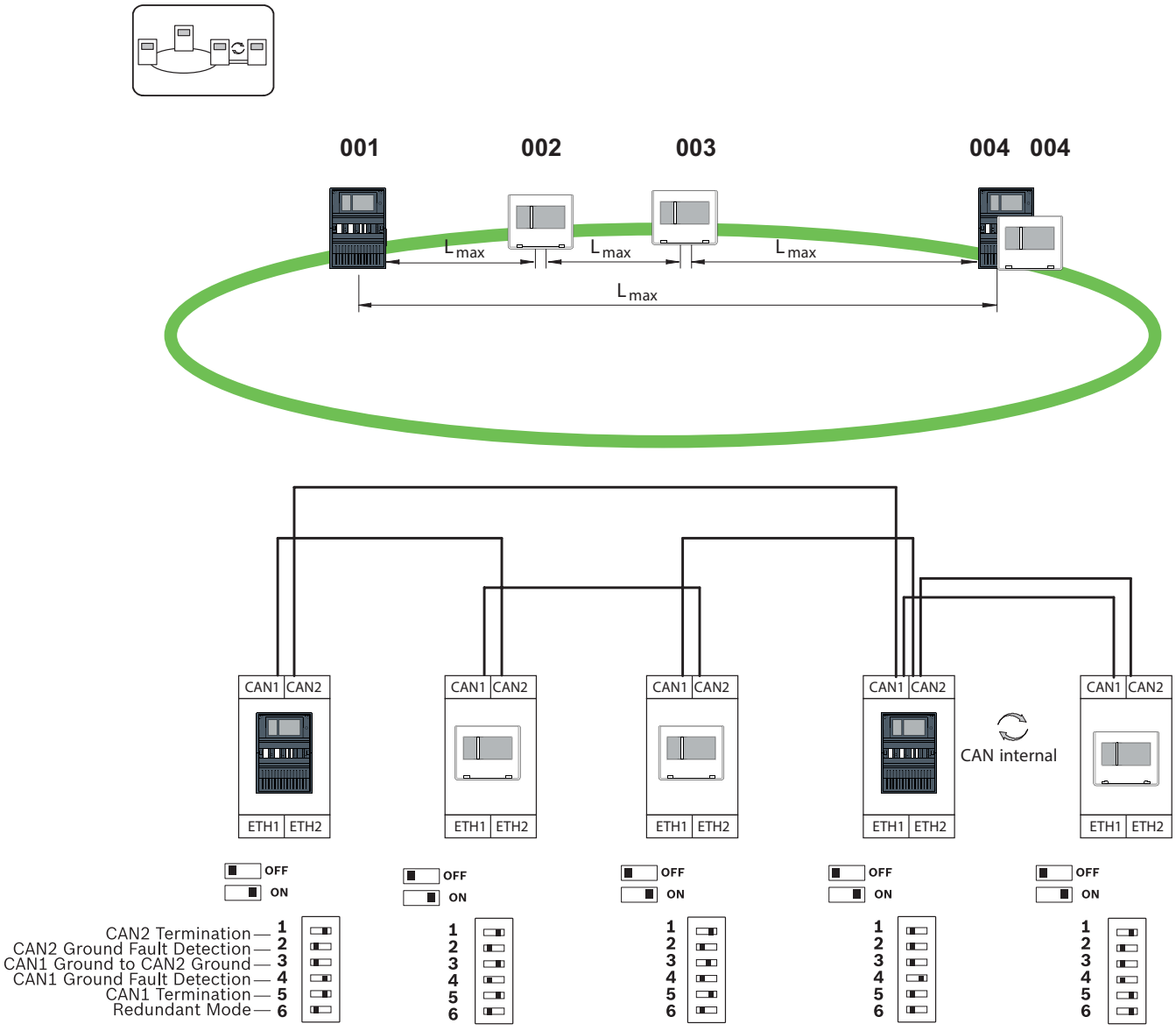


Figura 10.5: Definições do interruptor DIP para loop com painel repetidor (apenas AVENAR)

11 Cablagem

Para criar um sistema em conformidade com a norma EN 54-2, ligue os switches RSTP e os conversores multimédia através da fonte de alimentação monitorizada do painel de controlo do alarme de incêndio.

- Para a fonte de alimentação dos conversores multimédia e switches RSTP, utilize a saída de 24 V do BCM 0000 B ou do FPP-5000.
- As saídas de falha do switch RSTP têm de monitorizadas através das entradas do painel se tiver ligado uma fonte de alimentação redundante ou se estiver a criar uma ligação de switch a switch. Por exemplo, utilize as entradas no painel de controlo ou IOP 0008 A.
- No caso do conversor multimédia, a função Link Fault Pass-Through deve estar ativada. A configuração é realizada através do interruptor DIP do conversor multimédia.

Informação!
Utilize sempre os seguintes cabos na ligação em rede:
Cabo Ethernet
Cabo de rede Ethernet, blindado, CAT5e ou superior.
Tenha em atenção os raios de curvatura mínimos indicados na especificação do cabo.
Cabo de fibra ótica
Modo múltiplo: cabo de rede Ethernet de fibra ótica, I-VH2G 50/125µ duplex ou I-VH2G 62.5/125µ duplex, ficha SC.
Modo único: cabo de rede Ethernet de fibra ótica, I-VH2E 9/125µ duplex, ficha SC.
Tenha em atenção os raios de curvatura mínimos indicados na especificação do cabo.

11.1 Conversor multimédia

Ligação de conversores multimédia

Informação!
Tenha em atenção a direção de transmissão das fibras FOC quando ligar a cablagem FX dos conversores multimédia.

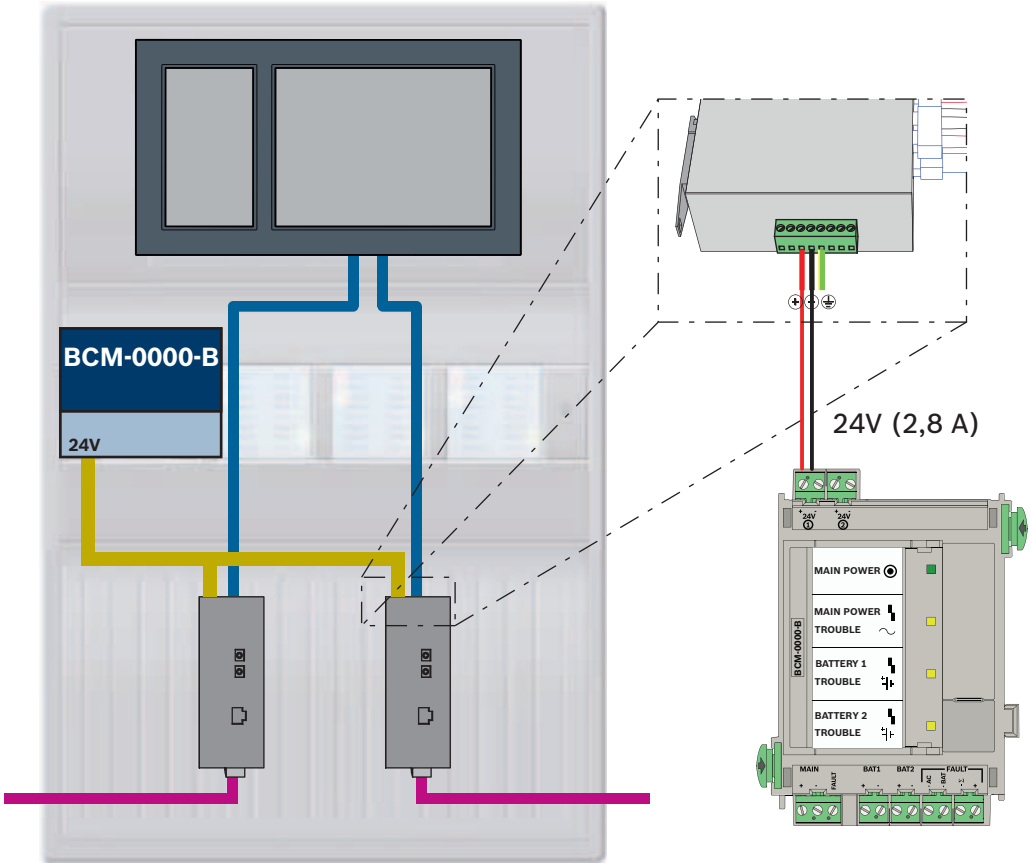


Figura 11.1: Ligação do conversor multimédia à fonte de alimentação e ao painel de controlo IN1/IN2

Ícone	Descrição
	Cabo Ethernet TX (cobre)
	Cabo Ethernet FX (cabo de fibra ótica)
	Fonte de alimentação de 24 V

Ícone	Descrição
	Transmissão de falha
	Conversor multimédia

11.2 Switch Ethernet

Ligação do switch

Pode ligar as saídas de falha dos switches às entradas do painel de controlo ou a um módulo de entrada e saída IOP.

Informação!

O relé de falha só tem de ser ligado em aplicações onde, pelo menos, um dos seguintes requisitos esteja preenchido:

Existe uma ligação entre 2 switches. Isso é possível, por exemplo, no caso de uma infraestrutura com subloops.

A alimentação do switch é projetada de forma redundante.

Ligação de switches com comunicação de falhas às entradas do módulo IOP:

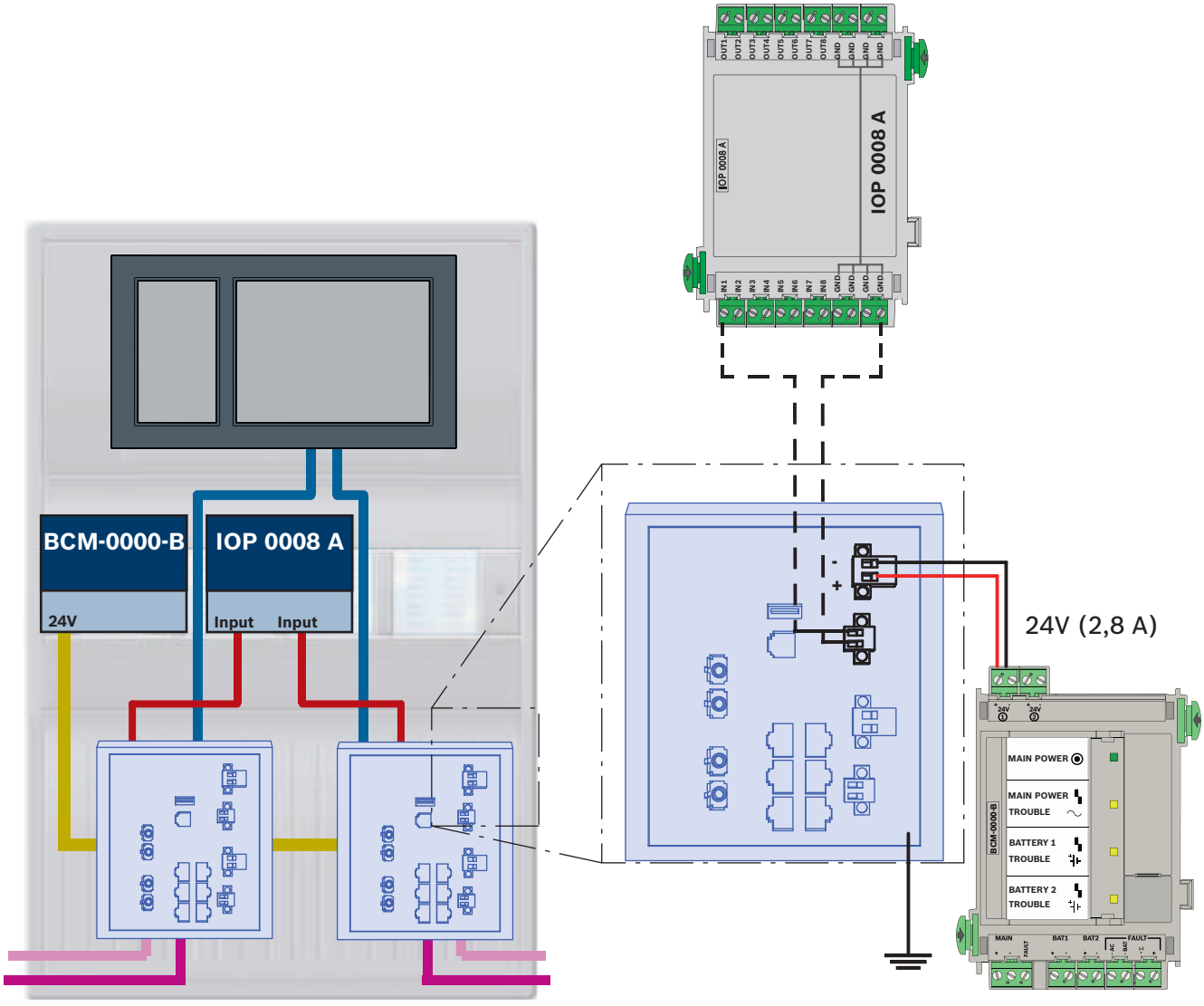


Figura 11.2: Ligação do switch à fonte de alimentação e ao IOP

Ícone	Descrição
	Cabo Ethernet TX (cobre)
	Cabo Ethernet FX (cabo de fibra ótica)
	Fonte de alimentação de 24 V
	Transmissão de falha
	Switch RSTP

Ligação de switches com comunicação de falhas às entradas do painel de controlo

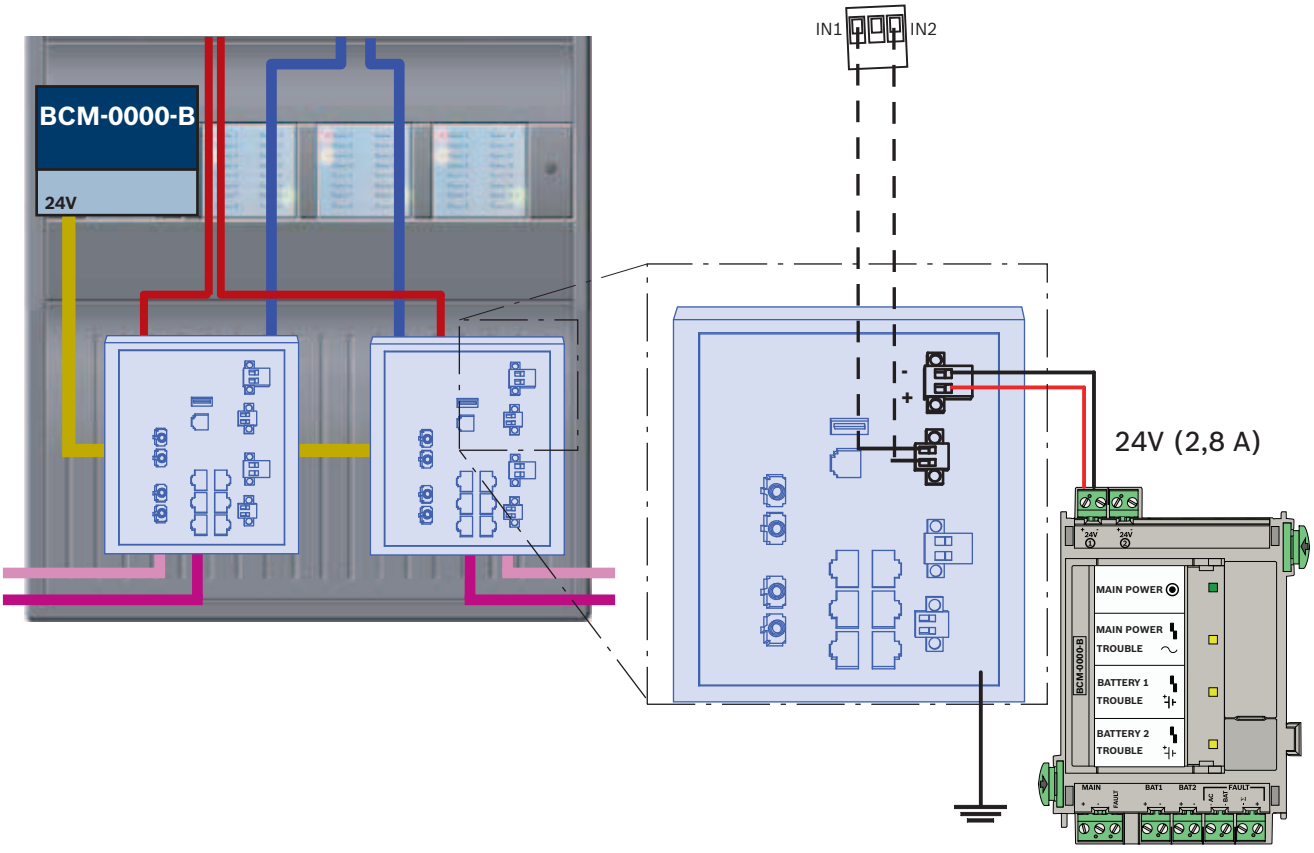
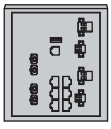


Figura 11.3: Ligação do switch à fonte de alimentação e ao painel de controlo

Ícone	Descrição
	Cabo Ethernet TX (cobre)
	Cabo Ethernet FX (cabo de fibra ótica)
	Fonte de alimentação de 24 V
	Transmissão de falha
	Switch RSTP

Informação!
Não utilize o cabo de rede fornecido para ligar os interruptores.
Utilize um cabo de rede Ethernet, blindado, CAT5e ou superior.

11.3 Painel repetidor

Um painel repetidor tem de ser alimentado por uma fonte de alimentação externa FPP-5000. A ligação à rede é estabelecida através de 2 conversores multimédia num PSS 0002 A ou num USF 0000 A.

Informação!
Tenha em atenção que a alimentação externa FPP-5000 e o PSF 0002 A (PSS 0002 A) devem ser instalados nas imediações (sem espaço intermédio) do painel repetidor. Não deve ser possível tocar nos cabos de ligação entre os componentes, uma vez que não são monitorizados relativamente a curtos-circuitos crescentes e monitorização aberta crescente.

Informação!
Utilize apenas conversores multimédia para ligar um Painel repetidor a uma rede de painéis Ethernet.
A utilização de switches não é permitida no Painel repetidor.

Informação!
A ligação à terra funcional do Painel repetidor tem de ser sempre aplicada quando ligar a unidade a uma rede de painéis Ethernet.

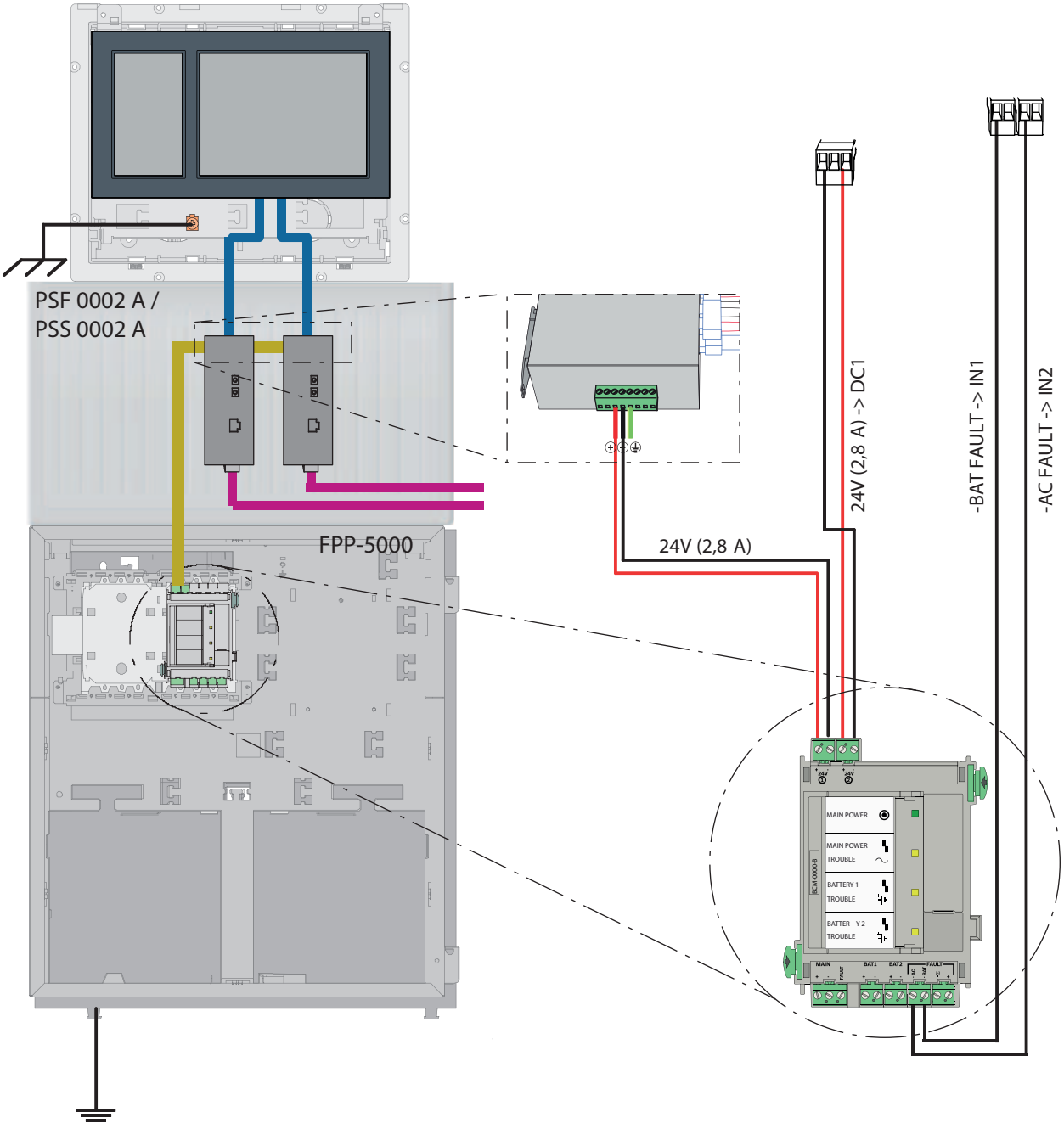


Figura 11.4: Cablagem do Painel repetidor

Ícone	Descrição
	Cabo Ethernet TX (cobre)
	Cabo Ethernet FX (cabo de fibra ótica)
	Fonte de alimentação de 24 V
	Conversor de multimédia

12 Definições do FSP-5000-RPS

É possível programar toda a rede com o software de programação RPS através da porta USB, da interface de rede ou da interface em série de um painel. Para o fazer, é necessário configurar as definições da rede no painel e reiniciá-la para poder colocar a rede em funcionamento.
Em alternativa, pode igualmente utilizar a interface de rede de um switch ligado à rede.

12.1 Nós de rede

Tem de programar toda a rede com todos os nós de rede no software de programação FSP-5000-RPS e transferir estes dados (upload) de programação para a rede. Para o fazer, prossiga da seguinte forma:

- Ligue os nós FPA
  - Defina o RSN nos nós individuais
- Ajuste os números de linha da cablagem da rede de modo a criar a topologia planeada
- Verifique a visualização da topologia de modo a garantir que a topologia está correta
- Sempre que necessário, ligue o servidor OPC, o sistema de alarme por voz, o servidor UGM-2040 e os switch
- Edite a configuração IP e Ethernet
  - Atribua endereços IP ou utilize as definições padrão se estiver a utilizar uma topologia com menos de 20 switches RSTP
  - Escolha o protocolo de redundância adequado para a topologia definida
- Faça a verificação da consistência
- Ligue à rede através da Ethernet, de USB ou da interface em série
- Conclua um início de sessão múltiplo
- Execute uma deteção automática completa para cada painel
- Peça informações sobre a configuração e conclua todas as tarefas

Verifique as mensagens de erro após o reinício da rede e retifique quaisquer erros, se necessário.

12.2 Números de linha

Tem de atribuir um número de linha a cada ligação à rede utilizada. É irrelevante se se trata de uma ligação CAN ou de uma ligação Ethernet.
É possível utilizar um número de linha tanto para uma ligação CAN como para uma ligação Ethernet. Contudo, para obter uma melhor perspetiva das ligações, deve utilizar intervalos de números diferentes.
Considere que, se utilizar **Rede (network)** como **Tipo de Linha** na janela **Interface de rede**, o número de linha tem de ser 0 para todas as ligações.

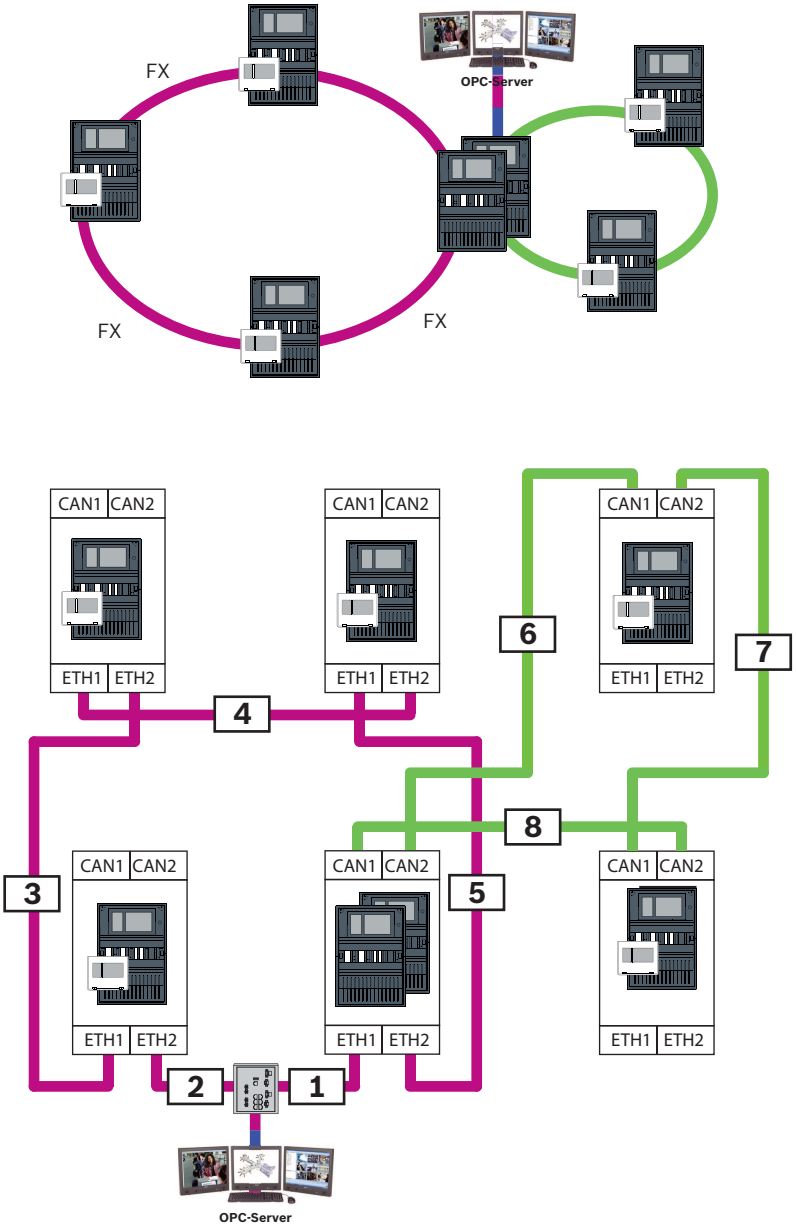


Figura 12.1: Exemplo de uma rede e a numeração de linhas possível

12.3 Interruptores

Se estiver a utilizar switches na rede, tem de criar estes switches no software de programação FSP-5000-RPS. Pode atribuir até 128 portas a cada switch criado. Para criar a rede, pode atribuir os números de linha ligados às portas individuais.

12.4 Servidores OPC

Os servidores OPC da sua rede devem ser adicionados ao software de programação FSP-5000-RPS.

Tem de efetuar as seguintes definições tanto no software FSP-5000-RPS como no servidor OPC:

- Nós de rede
- Grupo de rede
- RSN
- Endereço IP

– Porta

O servidor OPC utiliza a porta 25000 como padrão.

Informação!

EN 54

A ligação de um sistema de gestão de edifícios (por exemplo, BIS) através de uma interface Ethernet com um servidor OPC ou um servidor FSI cumpre os requisitos da norma EN54 desde que as funções relevantes da EN54 sejam realizadas apenas pelo painel de incêndio. Qualquer controlo ou administração relevante da EN54 (por exemplo, controlo de aparelhos de notificação ou administração de desativação) pelo sistema de gestão de edifícios requer uma certificação EN54 individual do sistema em geral por um organismo de certificação.

Informação!

Software de programação FSP-5000-RPS

Tem de atribuir um servidor OPC a cada nó da rede a partir do qual os estados devem ser transmitidos.

12.5 Servidores UGM-2040

Informação!

Todos os painéis de controlo e os servidores UGM têm de estar localizados na mesma sub-rede e ter o mesmo endereço multicast.

No caso de existirem múltiplas redes ou configurações de painéis, estas têm de estar localizadas na mesma sub-rede. Os endereços multicast têm de ser diferentes.

Informação!

Tem de atribuir o servidor UGM-2040 a cada nó da rede a partir do qual os estados devem ser transmitidos.

Para ligar um painel ao UGM-2040, tem de simular a estrutura física da rede no RPS. Isso também inclui os números de linha entre o painel de controlo de ligação e os switches do UGM-2040.

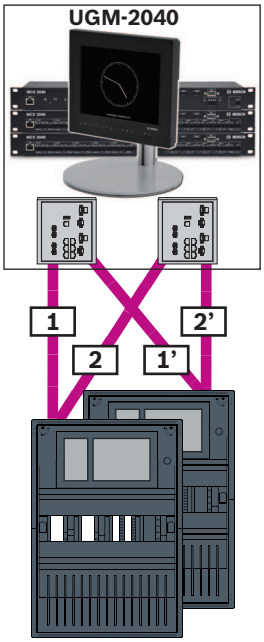


Figura 12.2: Exemplo de numeração de linhas para o UGM-2040

13 Apêndice

13.1 Mensagens de erro da Ethernet

Tenha em atenção que, se ocorrer um erro, a mensagem de erro e o grupo do erro serão apresentados em cada instância.

Endereço físico	Endereço lógico	Mensagem de erro	Descrição e causa possível
Falhas de grupo relacionadas com uma falha geral da rede			
135.0.1.0	Rede 1.0	**Anomalia geral de rede**	Existe uma versão incompatível do software da rede de painéis. Existem 2 versões de software diferentes
Falhas de grupo relacionadas com a rede			
135.0.6.1	Rede 2.1	**Endereço IP duplicado**	Um endereço IP foi atribuído duas vezes.
135.0.6.2	Rede 2.2	**Definições de IP**	A configuração IP do painel a comunicar é diferente da configuração RPS
135.0.6.3	Rede 2.3	**Definições de redundância**	A configuração de redundância (RSTP, parâmetro RSTP, homing duplo ou um valor nulo) do painel a comunicar é diferente da configuração RPS.
Falhas de grupo relacionadas com o protocolo RSTP (Rapid Spanning Tree Protocol)			
135.0.7.1	Rede 3.1	**RSTP Fallback**	O painel a comunicar mudou do modo RSTP para o modo STP (modo de compatibilidade). Um dispositivo STP foi ligado à rede.
135.0.7.2	Rede 3.2	**Alteração de topologia RSTP**	A topologia de rede RSTP foi alterada. Por exemplo, foi adicionado outro dispositivo RSTP à rede. Esta mensagem pode igualmente ser apresentada se houver uma interrupção na linha.

Endereço físico	**Endereço lógico**	**Mensagem de erro**	**Descrição e causa possível**
135.0.7.3	Rede 3.3	**Ligação RSTP de tipo ponto-a-ponto**	Uma porta RSTP do painel a comunicar não está no estado ponto a ponto. Por exemplo, foram ligados vários dispositivos RSTP a uma porta RSTP. Em alternativa, foi ligado outro dispositivo RSTP à porta RSTP através de uma linha half-duplex.
Falhas de grupo relacionadas com a ligação de rede			
135.0.5.1	Ligação de rede 1.0	**Anomalia da CAN 1**	A transmissão de dados ao bus CAN 1 está restringida. Possíveis causas são: ruturas de cabo, cabo não ligado, interferência no cabo.
135.0.5.2	Ligação de rede 2.0	**Anomalia da CAN 2**	A transmissão de dados ao bus CAN 2 está restringida. Possíveis causas são: ruturas de cabo, cabo não ligado, interferência no cabo.
135.0.5.3	Ligação de rede 3.0	**Anomalia de Ethernet 1**	A transmissão de dados à linha Ethernet 1 está restringida. Possíveis causas são: ruturas de cabo, cabo não ligado, interferência no cabo.
135.0.5.4	Ligação de rede 4.0	**Anomalia de Ethernet 2**	A transmissão de dados à linha Ethernet 2 está restringida. Possíveis causas são: ruturas de cabo, cabo não ligado, interferência no cabo.

Índice remissivo

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

Building solutions for a better life.

202202161639