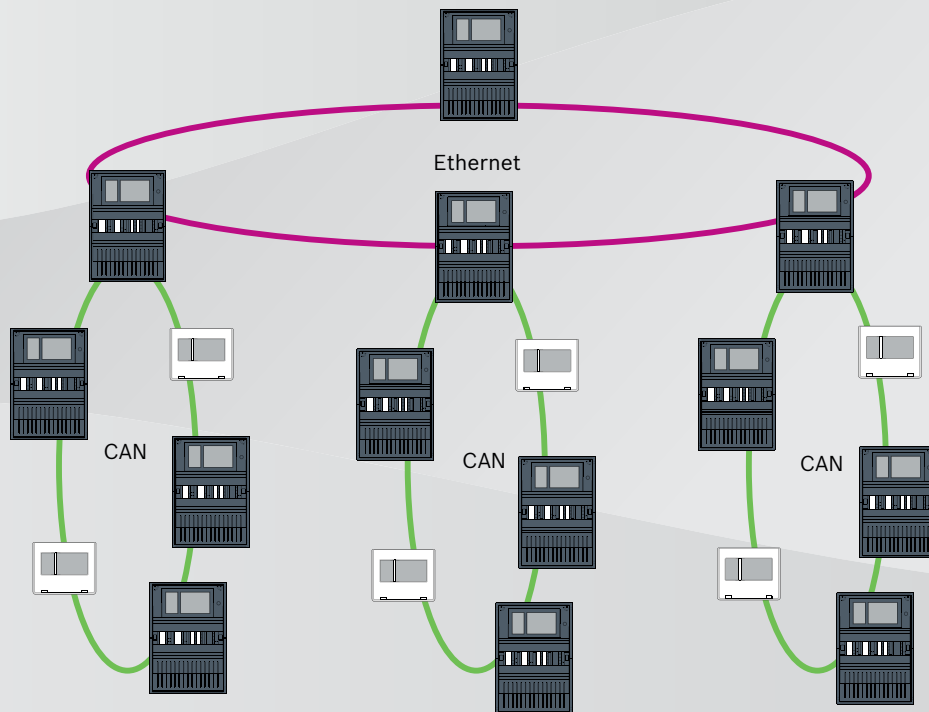


AVENAR panel serie | FPA-5000 | FPA-1200



Sommaro

1	Sicurezza	5
1.1	Misure organizzative per PC che eseguono client di servizio	5
1.2	Spiegazione dei simboli di sicurezza	6
1.3	Avvisi di sicurezza	6
2	Introduzione	8
3	Panoramica sistema	8
4	Topologie	10
4.1	Loop CAN	15
4.2	Loop Ethernet	15
4.3	Loop Ethernet con server OPC	16
4.4	Loop Ethernet con server OPC su centrale ridondante	16
4.5	Loop doppio CAN/Ethernet	17
4.6	Loop CAN con segmenti Ethernet	17
4.7	Anello principale Ethernet con loop secondari (Ethernet/CAN)	17
4.8	Collegamento dei loop Ethernet	19
5	Rete Ethernet	21
5.1	Protocolli	21
5.2	Diametro della rete	22
5.3	Cavi utilizzati	24
5.4	Creazione o modifica di una rete Ethernet	25
6	Rete CAN	26
6.1	Creazione o modifica di una rete CAN	28
7	Modello di collegamento in rete Ethernet e CAN	28
7.1	Rete di centrali su Ethernet	30
7.2	Rete di centrali su CAN	30
7.3	Connessione dei servizi alla centrale	31
7.4	Rete di centrali su Ethernet con centrali ridondanti	32
7.5	Rete di centrali su CAN con centrali ridondanti	32
7.6	Rete di centrali su due loop Ethernet	33
7.7	Rete di centrali su due loop Ethernet con centrali ridondanti	33
7.8	Connessione di reti Ethernet e CAN con centrali ridondanti	33
7.9	Connessione di servizi remoti a centrali ridondanti	34
8	Remote Services	34
8.1	Remote Connect	35
8.2	Remote Alert	36
8.3	Remote Maintenance	37
8.4	Remote Portal	39
9	Sistemi di allarme vocale	41
10	Installazione	42
10.1	Impostazioni del media converter	43
10.2	Installazione dello switch Ethernet	44
10.3	Impostazioni dello switch	44
10.3.1	Assegnare l'indirizzo IP	45
10.3.2	Programmazione delle impostazioni di ridondanza	45
10.3.3	Programmazione del relè di guasto	46
10.3.4	Programmazione del monitoraggio dei collegamenti	47
10.3.5	Priorità QoS, solo per UGM-2040	47
10.3.6	Attivazione dello snooping IGMP	47

10.4	Rete CAN	48
11	Cablaggio	53
11.1	Convertitore di supporti	54
11.2	Switch Ethernet	55
11.3	Tastierino remoto	58
12	Impostazioni FSP-5000-RPS	60
12.1	Nodi di rete	60
12.2	Numeri delle linee	60
12.3	Switch	61
12.4	Server OPC	61
12.5	Server UGM-2040	62
13	Appendice	63
13.1	Messaggi di errore Ethernet	63
	Indice	65

1 Sicurezza

Questo capitolo illustra le misure organizzative per i PC che eseguono client di servizio per il portafoglio di prodotti antincendio Bosch. È obbligatorio rispettare tali accordi contrattuali. Il capitolo include anche avvisi di sicurezza, raccolti e ordinati per argomento. Più avanti, gli avvisi di sicurezza sono anteposti alle istruzioni correlate.

1.1 Misure organizzative per PC che eseguono client di servizio

Introduzione

Il portafoglio di prodotti antincendio Bosch comprende programmi per PC (client di servizio) in esecuzione su computer che richiedono un collegamento fisico al sistema di rivelazione incendio. Per motivi di sicurezza e per soddisfare i requisiti normativi standard, il sistema di rivelazione incendio non deve essere installato in una rete condivisa. Ciò significa che l'intera rete del sistema di rivelazione incendio e il PC che esegue un client di servizio devono costituire una rete fisica dedicata. Poiché Bosch sviluppa i client di servizio ma non i PC in cui vengono eseguiti, il computer non è sotto il controllo di Bosch. Il presente documento illustra le misure organizzative necessarie per ridurre il rischio di problemi di sicurezza.

Misure

Se le misure descritte di seguito richiedono una connessione a Internet o il client di servizio richiede una connessione a Internet temporanea in relazione alla licenza, il PC deve essere fisicamente isolato dalla rete del sistema di rivelazione incendio prima di connettere il PC a Internet. La connessione a Internet deve essere rimossa prima di collegare nuovamente il PC alla rete di sistema di rivelazione incendio.

1. Sistemi operativi

Bosch documenta i prerequisiti per i client di servizio, incluse le versioni dei sistemi operativi. La compatibilità dei client con tali versioni è garantita. Il sistema operativo in cui il client è in esecuzione deve essere aggiornato regolarmente per correggere potenziali vulnerabilità di sicurezza.

Il sistema deve essere configurato in modo da consentire l'accesso in scrittura solo alle cartelle necessarie per la relativa attività. Per impostazione predefinita, a tutti gli utenti vengono concesse autorizzazioni di sola lettura.

2. Antivirus

Nel computer è necessario installare ed eseguire un software antivirus all'avanguardia. I relativi file delle definizioni devono essere aggiornati regolarmente.

3. Firewall

Nel computer è necessario installare ed eseguire un software firewall. Deve essere configurato per consentire il traffico tra il client di servizio e il sistema di rivelazione incendio e gli aggiornamenti del sistema operativo e del software antivirus. Tutto il resto del traffico deve essere bloccato.

4. Accesso utente sicuro

L'accesso al PC deve essere limitato agli operatori che utilizzano il client di servizio installato. L'accesso deve essere protetto con strumenti all'avanguardia. Se si sceglie una password per proteggere l'accesso, è necessario applicare criteri per regole password all'avanguardia.

Ove applicabile, è consigliabile adottare un approccio all'autenticazione a due persone o a più fattori.

5. Software e servizi

Il numero di software installati nel PC deve essere ridotto al minimo. Installare solo il software necessario per le attività corrispondenti e per il client di servizio.

6. Limiti di utilizzo
L'utilizzo del PC deve essere limitato alle attività relative al servizio mediante strumenti dell'organizzazione. Ciò comprende anche l'uso di Internet per scopi diversi da quelli descritti nel presente documento.
7. Separazione dei compiti
I compiti e le aree di responsabilità devono essere separati per ridurre il rischio di modifiche non autorizzate o utilizzi accidentali. Vale a dire che ai vari ruoli vanno assegnati compiti diversi.
8. Monitoraggio
È necessario monitorare tutti i tentativi di accesso al PC che esegue il client di servizio per riconoscere gli accessi non autorizzati al PC e a Internet.

1.2 Spiegazione dei simboli di sicurezza



Avvertenza!

Indica una situazione pericolosa che, se non evitata, può causare lesioni gravi o mortali.



Attenzione!

Indica una situazione pericolosa che, se non evitata, può causare lesioni di lieve o media entità.



Avviso!

Indica una situazione che, se non evitata, può causare danni all'apparecchiatura o all'ambiente oppure la perdita di dati.

1.3 Avvisi di sicurezza

Media converter



Avvertenza!

Luce laser

Non guardare in direzione del fascio ad occhio nudo o con strumenti visivi di qualunque tipo (ad es. lente di ingrandimento, microscopio). L'inosservanza di questo avviso costituisce un pericolo per gli occhi a una distanza inferiore a 100 mm. La luce emerge all'altezza dei terminali video o all'estremità dei cavi in fibra ottica ad essi collegati. Diodo laser CLASSE 2M, lunghezza d'onda 650 nm, uscita < 2 mW, in conformità alla normativa IEC 60825-1.

Remote Services



Attenzione!

Per l'accesso via Internet, utilizzare solo BoschRemote Services.

**Attenzione!**

Remote Services richiede una connessione IP protetta. È necessario utilizzare Bosch Remote Services o una connessione con Private Secure Network.

Private Secure Network viene fornito con una rete IP basata su DSL, con accesso wireless opzionale sul lato della centrale (EffiLink). Remote Services per Private Secure Network è disponibile solo in Germania con un contratto di assistenza con Bosch BT-IE.

**Avviso!**

Per effettuare una configurazione di una rete di allarme incendio centrale è necessaria una rete Ethernet dedicata.

L'utente si assume il rischio di utilizzare un sistema di rivelazione incendio in qualsiasi altra rete Ethernet. Bosch esclude qualsiasi garanzia e responsabilità per questa applicazione scorretta.

In caso di rete Ethernet non esclusiva, la sicurezza IT e la trasmissione degli allarmi affidabile non può essere garantita.

Rete di centrali**Avviso!**

EN 54

Per assicurarsi che la rete venga configurata in conformità allo standard EN 54, utilizzare esclusivamente componenti approvati per l'uso nelle reti di allarme incendio centrali.

Gli switch RSTP esterni ed i media converter nelle reti Ethernet devono essere installati in alloggiamenti centrale. L'installazione all'esterno dell'alloggiamento centrale non è conforme allo standard EN 54.

**Avviso!**

Lunghezza cavo TX

Tutte le connessioni IP devono essere dirette o tramite media converter approvati da Bosch. La lunghezza da nodo a nodo del cavo TX deve essere inferiore a 100 m.

**Avviso!**

VdS 2540

Per soddisfare i requisiti delle linee guida VdS 2540 per i percorsi di trasmissione dati, utilizzare un cavo in fibra ottica per le connessioni Ethernet. Per i collegamenti all'interno dell'alloggiamento è possibile utilizzare cavi Ethernet TX.

**Avviso!**

Per le applicazioni standard, utilizzare le impostazioni di rete standard.

Le modifiche alle impostazioni di rete standard sono riservate esclusivamente agli utenti esperti con competenze adeguate in materia di collegamenti in rete.

**Avviso!**

Topologie applicabili

La funzionalità e la comunicazione tra le centrali sono limitate dal tipo di centrale. Fare riferimento alle specifiche della centrale per informazioni sui servizi e il numero di centrali e tastierini remoti collegabili.

2 Introduzione

Questo documento è rivolto ai lettori con esperienza nella progettazione e nell'installazione di sistemi di rivelazione incendio conformi allo standard EN 54. Inoltre, è necessario disporre di competenze in materia di collegamenti in rete.

Questo documento illustra diverse topologie di rete degli allarmi incendio. Le topologie vengono descritte indipendentemente dal tipo di centrale antincendio.

Per creare reti di centrali corrispondenti alle topologie e ai servizi di connessione introdotti, è necessario attenersi al modello di collegamento in rete descritto in questo documento.

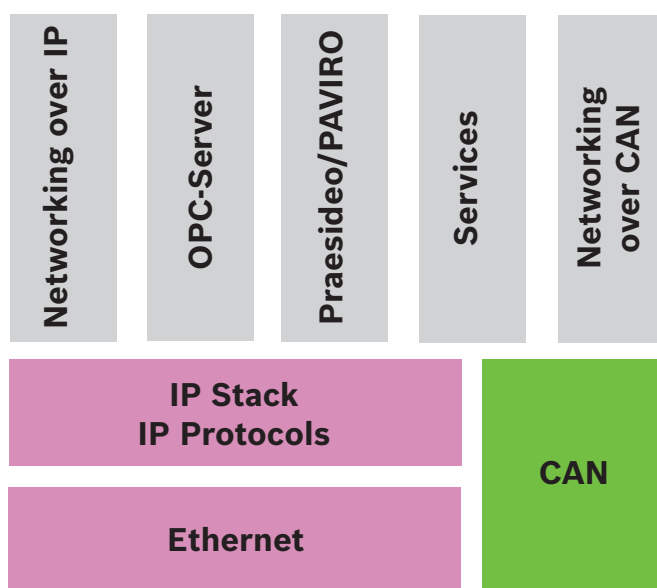
Il documento offre una panoramica delle condizioni di base, dei valori limite e delle procedure generali per la progettazione e l'installazione di una rete di centrali.

Le descrizioni dettagliate dell'installazione dei singoli componenti sono riportate nelle rispettive guide all'installazione.

Per una descrizione dell'interfaccia utente dell'unità di controllo della centrale, consultare la guida utente in dotazione con il dispositivo.

L'interfaccia utente del software di programmazione di FSP-5000-RPS è illustrata nella guida in linea.

3 Panoramica sistema



Nella rete, l'interfaccia Ethernet ed i protocolli IP vengono utilizzati per servizi differenti. L'interfaccia Ethernet può essere disattivata completamente oppure può esserne disattivato l'utilizzo solo per il collegamento in rete su TCP/IP. Per il collegamento in rete su CAN può essere necessario disabilitare l'interfaccia.

Abilitazione dei servizi

- Collegamento in rete su TCP/IP
In FSP-5000-RPS, è possibile abilitare la comunicazione tra centrali nella rete Ethernet
- Server OPC
È possibile aggiungere un server OPC alla configurazione FSP-5000-RPS
- Connessione Praesideo/PAVIRO
È possibile aggiungere un sistema di allarme vocale alla configurazione FSP-5000-RPS e configurare i trigger virtuali
- Remote Services (Remote Connect come prerequisito, Remote Maintenance e Remote Alert)
È possibile attivare la casella di controllo corrispondente in FSP-5000-RPS

- Remote Services (Remote Connect come prerequisito, Remote Maintenance e Remote Alert) per Private Secure Network
È possibile aggiungere l'accesso remoto alla configurazione FSP-5000-RPS e configurare l'accesso remoto in FSP-5000-RPS



Avviso!


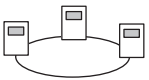

Trasferimento dati accidentale


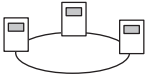
Se l'interfaccia Ethernet dell'unità di controllo della centrale viene utilizzata solo per la comunicazione con un server OPC o per Remote Services disattivare la comunicazione della centrale mediante TCP/IP, in FSP-5000-RPS. Altrimenti, è possibile che vi sia una trasmissione accidentale di dati di incendio via Ethernet.


Per utilizzare i servizi Ethernet o TCP/IP è necessario che le interfacce Ethernet vengano attivate e vengano configurate le impostazioni TCP/IP corrette.

Rete di centrali e tastierini remoti

La tabella seguente mostra le opzioni disponibili per il collegamento in rete delle centrali/ tastierini remoti a seconda della topologia di rete e del tipo di centrale. Considerare i limiti stabiliti dalla topologia di rete.

Topologia	AVENAR panel 8000, licenza premium	AVENAR panel 8000, licenza standard	AVENAR panel 2000, licenza premium	AVENAR panel 2000, licenza standard
 Indipendente	Possibile	Possibile	Possibile	Possibile
 Loop	Max. 32 centrali/ tastierini remoti, connettività con AVENAR panel 2000, licenza premium e FPA	Max. 32 centrali/ tastierini remoti, connettività con AVENAR panel 2000, licenza premium e FPA	Max. 32 centrali/ tastierini remoti, connettività con AVENAR panel 8000 e FPA	1 centrale e max. 3 tastierini remoti
 Ridondanza della centrale	Anche l'unità di controllo della centrale ridondante deve essere premium. È anche possibile utilizzare un tastierino remoto come centrale ridondante.	L'unità di controllo della centrale ridondante può essere standard. È anche possibile utilizzare un tastierino remoto come centrale ridondante.	Impossibile	Impossibile

Topologia	FPA-5000	FPA-1200
 Indipendente	Possibile	Possibile
 Loop	Max. 32 centrali e tastierini remoti	1 centrale e max. 3 tastierini remoti

Topologia	FPA-5000	FPA-1200
 Ridondanza della centrale	Possibile	Impossibile (l'interruttore DIP 6 sull'unità di controllo della centrale non funziona)

Se si estende una rete FPA-5000, Bosch consiglia di utilizzare una centrale della serie AVENAR panel a tale scopo.

Quando si sostituisce una centrale della serie FPA con una della serie AVENAR panel, è sufficiente sostituire soltanto l'unità di controllo della centrale. Ricordare che le centrali della serie AVENAR panel non supportano le schede indirizzi. Nel caso di uno switch Ethernet collegato, è possibile continuare a utilizzarlo.

Quando si sostituisce un tastierino remoto della serie FPA con uno della serie AVENAR panel, verificare se la resistenza di linea è compresa nell'intervallo specificato per il tastierino remoto della serie AVENAR panel.

Avviso!

Installazione del firmware

Le centrali collegate devono avere la stessa versione del firmware.

È possibile eseguire un'installazione firmware esclusivamente per la centrale attiva. Per le centrali ridondanti, è necessario eseguire l'installazione del firmware per entrambe le centrali. A tal fine, occorre commutare i ruoli della centrale e riportarli allo stato iniziale dopo l'installazione del firmware.



Avviso!

Unità di controllo della centrale ridondante

Non è possibile combinare una unità di controllo della centrale della serie AVENAR panel e una unità di controllo della centrale della serie FPA per la ridondanza.



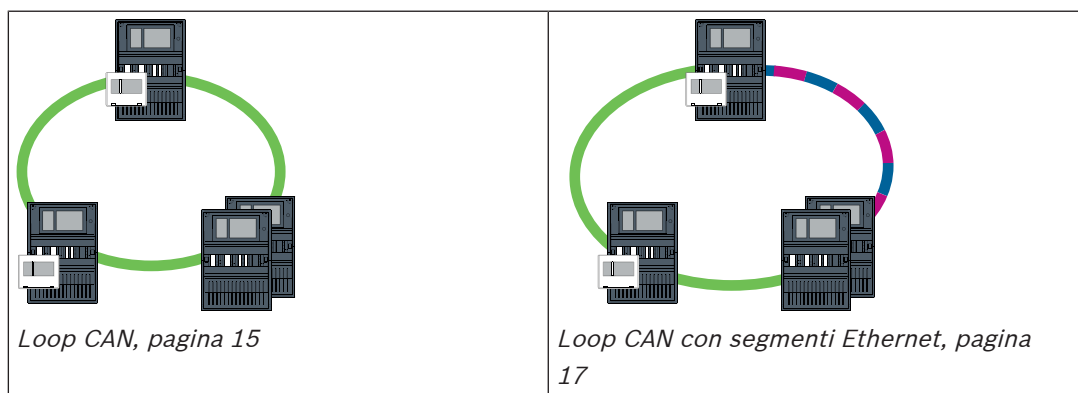
4 Topologie

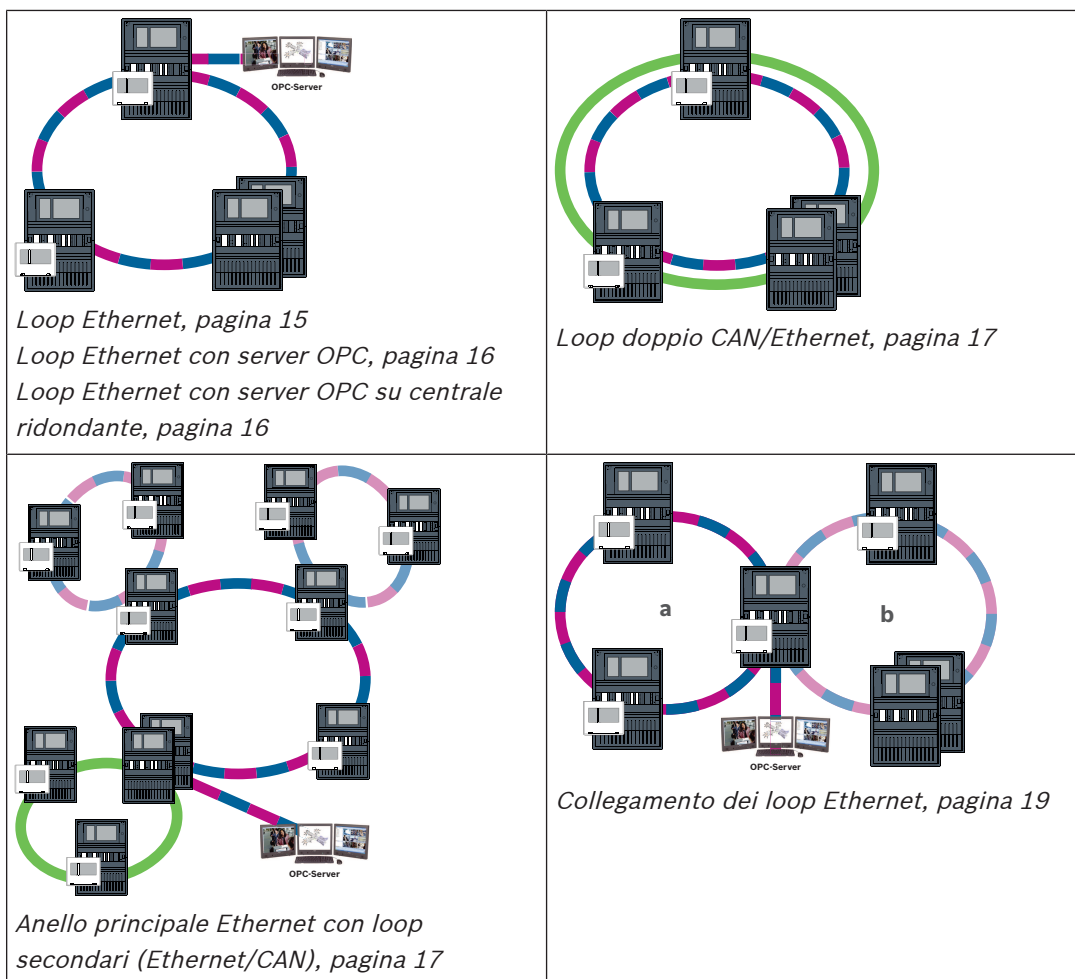
Questo documento illustra diverse topologie di rete degli allarmi incendio. Le topologie vengono descritte indipendentemente dal tipo di centrale antincendio.

Avviso!

Topologie applicabili

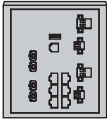


La funzionalità e la comunicazione tra le centrali sono limitate dal tipo di centrale. Fare riferimento alle specifiche della centrale per informazioni sui servizi e il numero di centrali e tastierini remoti collegabili.





Cavo	Descrizione
	Cavo Ethernet TX (in rame), lunghezza cavo TX da nodo a nodo < 100 m
	Cavo Ethernet FX (cavo in fibra ottica)
	Cavo Ethernet TX o FX, lunghezza cavo TX da nodo a nodo < 100 m
	Cavo CAN, lunghezza cavo CAN da nodo a nodo < 1000 m

Dispositivo	Descrizione
	Centrale o tastierino remoto (nella topologia Ethernet, uno switch RSTP interno ciascuno)
	Centrale ridondante (nella topologia Ethernet, switch RSTP interno) Un tastierino remoto può essere utilizzato come unità di controllo della centrale ridondante. Le connessioni di rete e le impostazioni per una unità di controllo della centrale ridondante e un tastierino ridondante sono identiche. L'utilizzo di un tastierino ridondante è applicabile unicamente a AVENAR panel 8000.

Dispositivo	Descrizione
	Switch Ethernet come switch RSTP esterno (in genere, switch Ethernet MM)
	Media converter
	Gateway di rete sicuro per Remote Services

Limiti della rete

Il numero di centrali e tastierini remoti collegabili in rete dipende dalla scelta della topologia di rete.

Le centrali ed i tastierini remoti collegati in rete vengono definiti nodi.

- Il numero di punti di rivelazione in una rete è limitato a 32768.
- Il numero di punti di rivelazione per centrale utilizzato in una rete è limitato a 2048.
- Il numero di nodi per sistema dipende dal tipo di topologia.
Nodo si riferisce sia a un'unità di controllo della centrale che a un tastierino remoto.
- Il numero di nodi in una topologia loop è limitato a 32.
- FSP-5000-RPS permette di assegnare un massimo di 3 tastierini remoti configurati a una centrale.

Il cablaggio tra i nodi e la lunghezza massima del cavo consentita vengono inoltre determinati dalla scelta della topologia.

È possibile combinare fino a 32 unità di controllo della centrale, tastiere remote e server OPC per formare una rete.

A seconda dell'applicazione prevista, unità di controllo della centrale e tastiere remote differenti possono essere suddivise in gruppi e definite come nodi di rete o nodi locali. In genere, all'interno di un dato gruppo, è possibile visualizzare solo lo stato delle centrali di controllo del gruppo specifico. È possibile visualizzare e/o elaborare lo stato di tutte le centrali di controllo dai nodi di rete, indipendentemente dal gruppo a cui appartengono.

Indirizzo del nodo fisico

Una centrale o un tastierino remoto viene identificato in rete da un indirizzo univoco, noto come indirizzo del nodo fisico.



Avviso!

Indirizzo del nodo fisico per centrali ridondanti

Una centrale ridondante deve avere lo stesso indirizzo del nodo fisico della centrale principale assegnata.



Avviso!

La rete in uso deve soddisfare i seguenti requisiti minimi:

Banda passante minima: 1 Mbps

Latenza massima: 250 ms

**Avviso!**

EN 54

Per assicurarsi che la rete venga configurata in conformità allo standard EN 54, utilizzare esclusivamente componenti approvati per l'uso nelle reti di allarme incendio centrali. Gli switch RSTP esterni ed i media converter nelle reti Ethernet devono essere installati in alloggiamenti centrale. L'installazione all'esterno dell'alloggiamento centrale non è conforme allo standard EN 54.

**Avviso!**

Centrale ridondante - EN 54-2

Per ciascuna centrale, è possibile collegare un massimo di 512 punti di rivelazione, in conformità allo standard EN 54-2. Se questo numero viene superato, la centrale deve essere progettata come ridondante.

Anche se la centrale funge da interfaccia con loop secondario CAN ed oltre 512 punti di rivelazione collegati nel loop secondario, questa deve essere progettata come ridondante. La ridondanza è affidata allo switch RSTP che collega 2 loop.

È possibile collegare fino a 4096 punti di rivelazione a una centrale autonoma, anche se progettata come ridondante. Se la centrale è inclusa in una rete, è possibile collegare un massimo di 2048 punti di rivelazione.

**Avviso!**

Verificare che l'indirizzo del nodo fisico assegnato alla centrale corrisponda a quello nel software di programmazione. Quest'ultimo è responsabile della definizione dell'ultimo numero dell'indirizzo IP nelle impostazioni standard.

Attivare RSTP come protocollo di ridondanza ed adottare i valori standard predefiniti.

Impostazioni Ethernet standard della centrale antincendio

Nelle impostazioni standard della centrale antincendio, sia il software di programmazione FSP-5000-RPS che l'unità di controllo adottano l'indirizzo del nodo fisico impostato come ultimo numero dell'indirizzo IP.

**Avviso!**

L'impostazione corretta dell'indirizzo del nodo fisico sulle unità di controllo della centrale e nel software di programmazione FSP-5000-RPS è un requisito per una rete operativa.

**Avviso!**

L'utilizzo della ridondanza Ethernet deve essere attivato separatamente nell'unità di controllo della centrale.

- Impostazioni IP
 - Indirizzo IP 192.168.1.x
L'ultima cifra dell'indirizzo IP nelle impostazioni standard corrisponde sempre all'indirizzo del nodo fisico impostato sull'unità di controllo della centrale.
 - Subnet mask 255.255.255.0
 - Gateway 192.168.1.254
 - Indirizzo multicast 239.192.0.1
 - Numero porta 25001 - 25008 (è possibile impostare solo la prima porta; vengono sempre utilizzate 8 porte consecutive)
- Parametri RSTP (impostazioni predefinite)

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



Avviso!

È possibile utilizzare le impostazioni standard della configurazione IP con reti che includono un massimo di 20 switch RSTP.

Nel caso di reti con oltre 20 switch RSTP, sono richieste impostazioni aggiuntive a seconda della topologia. Per questo, è richiesta la conoscenza approfondita delle reti.

Impostazioni per loop con oltre 20 switch RSTP

Se sono presenti oltre 20 switch RSTP nella rete, è necessario regolare le impostazioni RSTP sull'unità di controllo della centrale e nel software di programmazione. Le unità di controllo della centrale, i tastierini remoti e gli switch RSTP esterni collegati sono considerati switch RSTP. Le unità di controllo della centrale ridondanti non sono considerate switch RSTP, poiché l'interruttore contenuto in esse non è utilizzato come switch RSTP.

- Parametri RSTP
 - Mantenere Bridge Priority 32768
 - Mantenere Hello Time 2
 - Modificare Max. Age da 20 in 40
 - Modificare Forward Delay da 15 in 25

Parametri

- È possibile utilizzare massimo 32 nodi in un loop.
- Il diametro della rete non deve essere maggiore di 32; vedere *Diametro della rete*, pagina 22.
- Gli switch Ethernet non devono essere utilizzati all'esterno degli alloggiamenti centrale.
- I media converter non devono essere utilizzati all'esterno degli alloggiamenti centrale.

Caratteristiche

- La rete è conforme allo standard EN 54.
- La rete utilizza il protocollo RSTP.

Connessione a BIS con server OPC

Quando ci si collega ad un sistema di gestione edifici (BIS) tramite server OPC ed Ethernet 100BaseTX nelle reti estese a più edifici, è necessario chiarire con l'amministratore di rete se:

1. la rete è progettata per collegamenti su più edifici (ad es. non ci devono essere interferenze tecniche dovute a differenze nel potenziale di messa a terra);
2. la larghezza di banda degli utenti bus è sufficiente per la rete.

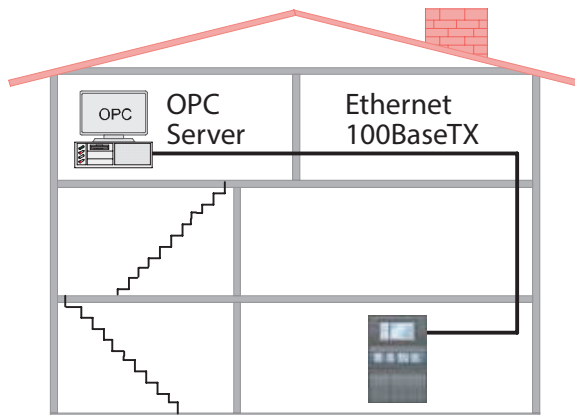


Figura 4.1: Connessione a BIS tramite server OPC

Informazioni aggiuntive per l'utilizzo di un server OPC

I server OPC nella rete devono essere aggiunti al software di programmazione FSP-5000-RPS. È necessario effettuare le seguenti impostazioni sia nel software FSP-5000-RPS che sul server OPC:

- Nodi di rete
- Gruppo di rete
- RSN
- Indirizzo IP
- Porta

Il server OPC utilizza la porta 25000 come standard.

Avviso!

EN 54

Il collegamento di un sistema di gestione edifici (ad esempio BIS) tramite un'interfaccia Ethernet utilizzando un server OPC o un server FSI è conforme a EN 54 se le funzioni relative a EN 54 vengono eseguite esclusivamente dalla centrale antincendio. Qualsiasi attività di controllo o amministrazione relativa a EN 54 (ad esempio il controllo degli apparecchi di notifica o l'amministrazione dello spegnimento) da parte del sistema di gestione edifici richiede una certificazione EN 54 individuale dell'intero sistema da parte di un ente di certificazione.



Avviso!

Software di programmazione FSP-5000-RPS

È necessario assegnare un server OPC a ciascun nodo di rete da cui vengono trasmessi gli stati.



4.1

Loop CAN

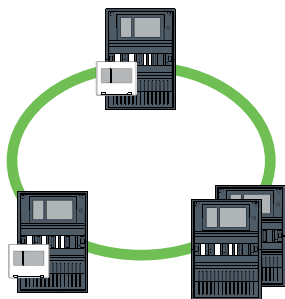


Figura 4.2: Loop CAN

4.2

Loop Ethernet

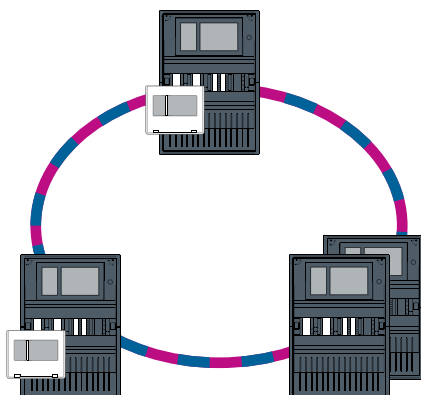


Figura 4.3: Loop Ethernet

4.3 Loop Ethernet con server OPC

Lo switch Ethernet per il collegamento del server OPC deve essere programmato separatamente

Programmare le impostazioni di ridondanza ed indirizzo IP dello switch Ethernet; vedere *Impostazioni dello switch, pagina 44*. Quando lo switch viene installato nelle immediate vicinanze (senza barriere intermedie), l'alimentazione non deve essere progettata come ridondante e le uscite di guasto non vengono pertanto utilizzate.

Verificare che le impostazioni RSTP nelle unità di controllo della centrale, nel software FSP-5000-RPS e nello switch Ethernet corrispondano.

Il server OPC deve essere programmato separatamente

Programmare l'indirizzo IP, i nodi di rete, il gruppo di rete e l'RSN. Vedere la sezione corrispondente nel capitolo Installazione della Guida al collegamento in rete.

Il server OPC utilizza la porta 25000 standard.

Verificare che le impostazioni nel software di programmazione FSP-5000-RPS e nel server OPC corrispondano.

Parametri

- È possibile collegare il server OPC tramite un cavo Ethernet (in rame) o un cavo in fibra ottica.

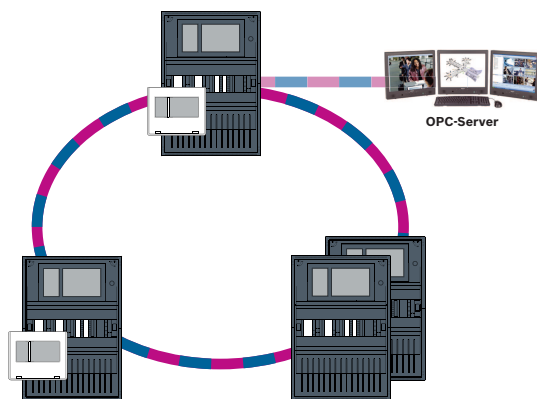


Figura 4.4: Loop Ethernet con server OPC

4.4 Loop Ethernet con server OPC su centrale ridondante

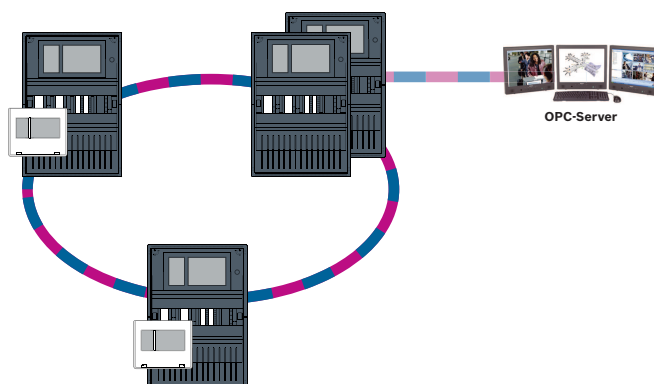


Figura 4.5: Loop Ethernet con server OPC su centrale ridondante

4.5 Loop doppio CAN/Ethernet

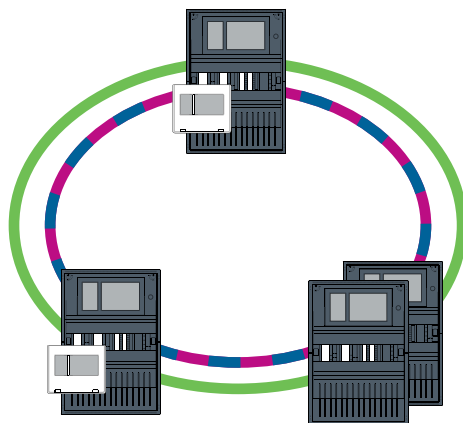


Figura 4.6: Loop doppio di Ethernet e CAN

4.6 Loop CAN con segmenti Ethernet

La topologia principale è un loop CAN. Quando la distanza tra due nodi è maggiore di 1.000 m, è possibile utilizzare una connessione Ethernet FX per coprire la distanza.

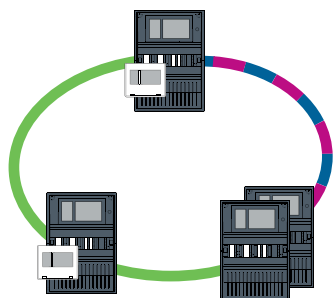


Figura 4.7: Loop CAN con segmenti Ethernet

4.7 Anello principale Ethernet con loop secondari (Ethernet/CAN)

Un anello principale Ethernet è collegato a tutti i loop secondari. Si tratta quindi di un'area di collegamento centrale con velocità di trasmissione dati elevate. Per impostazione predefinita, gli switch RSTP nell'anello principale non sono sopraordinati. Si noti che con questa topologia è necessario determinare il diametro della rete. Le unità di controllo della centrale, i tastierini remoti e gli switch RSTP esterni collegati sono considerati switch RSTP. Le centrali di rete CAN non vengono prese in considerazione ai fini del diametro della rete.

Prendere in considerazione le impostazioni per loop con oltre 20 switch RSTP; vedere *Impostazioni per loop con oltre 20 switch RSTP, pagina 14*.



Avviso!

Questa topologia richiede impostazioni aggiuntive per tutti gli switch RSTP dell'anello principale. Pertanto, è richiesta una conoscenza più approfondita delle reti.



Avviso!

Se la centrale funge da interfaccia con loop secondario CAN, questa centrale deve quindi essere progettata anche come ridondante, conformemente allo standard EN 54-2, se vengono collegati oltre 512 punti di rivelazione nel loop secondario.

Questa limitazione non è applicabile in un loop secondario Ethernet, poiché la ridondanza viene effettuata dagli switch di collegamento dei due loop.

Impostazioni aggiuntive

È necessario utilizzare il loop centrale come anello principale. Il collegamento in rete del loop centrale deve avvenire tramite Ethernet.

**Avviso!**

Per tutte le centrali e gli switch RSTP dell'anello principale, impostare una priorità RSTP più elevata rispetto ai loop secondari. In questo modo il ponte principale RSTP rimarrà sempre nell'anello principale, anche in caso di guasto.

Gli switch RSTP per il collegamento dei loop fanno parte dell'anello principale.

Utilizzare una priorità RSTP di 16384 nell'anello principale.

**Avviso!**

Minore è il valore impostato, maggiore sarà la priorità RSTP.

Gli switch per il collegamento del server OPC ed i loop secondari devono essere programmati separatamente

Programmare le impostazioni di ridondanza ed indirizzo IP degli switch Ethernet; vedere *Impostazioni dello switch, pagina 44*. Per questa topologia, le uscite di guasto dello switch devono essere utilizzate solo se l'alimentazione relativa allo switch stesso è stata progettata come ridondante o se esiste un collegamento tra switch; vedere *Switch Ethernet, pagina 55*. Verificare che le impostazioni RSTP nelle unità di controllo della centrale, nel software FSP-5000-RPS e nello switch Ethernet corrispondano.

**Avviso!**

Modificare la priorità RSTP degli switch RSTP che collegano i loop, poiché appartengono all'anello principale.

Il server OPC deve essere programmato separatamente.

Programmare l'indirizzo IP, i nodi di rete, il gruppo di rete e la RSN; vedere *Server OPC, pagina 61*.

Il server OPC utilizza la porta 25000 standard.

Verificare che le impostazioni nel software di programmazione RPS e nel server OPC corrispondano.

Parametri

- È possibile collegare il server OPC tramite un cavo Ethernet (in rame) o un cavo in fibra ottica.

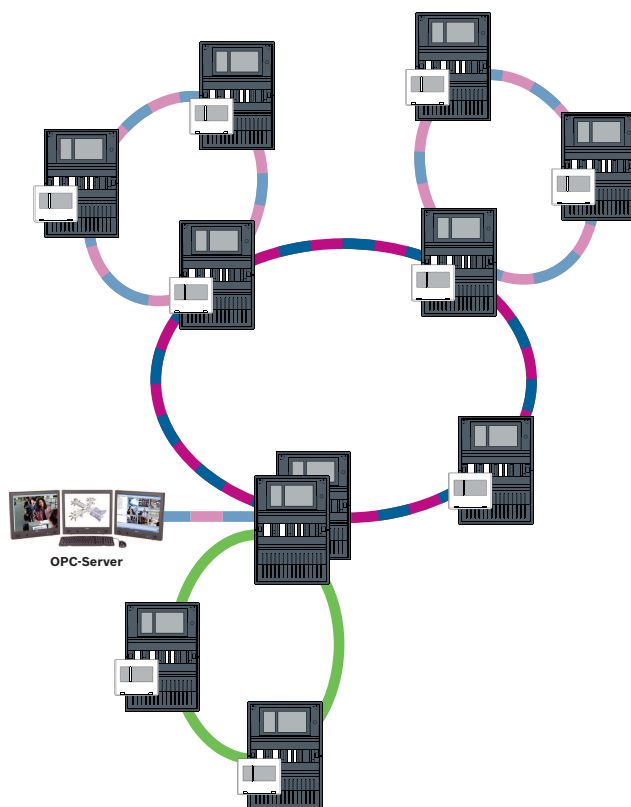


Figura 4.8: Anello principale Ethernet con loop secondari

4.8

Collegamento dei loop Ethernet



Avviso!

Questa topologia richiede impostazioni aggiuntive per tutti gli switch RSTP dell'anello principale. Pertanto, è richiesta una conoscenza più approfondita delle reti.

Impostazioni aggiuntive

Questa topologia è un'istanza speciale dell'anello principale Ethernet con loop secondari; vedere Anello principale in Ethernet con loop secondari (Ethernet/CAN). È necessario utilizzare uno dei due loop come anello principale.



Avviso!

Per tutte le centrali e gli switch dell'anello principale, impostare una priorità RSTP più elevata rispetto ai loop secondari. In questo modo il ponte principale RSTP rimarrà sempre nell'anello principale, anche in caso di guasto.

Gli switch per il collegamento dei due loop fanno parte dell'anello principale. Utilizzare una priorità RSTP di 16384 nell'anello principale.



Avviso!

Minore è il valore impostato, maggiore sarà la priorità RSTP.

Gli switch per il collegamento del server OPC ed il secondo loop devono essere programmati separatamente

Programmare le impostazioni di ridondanza ed indirizzo IP dello switch Ethernet; vedere *Impostazioni dello switch, pagina 44*. Per questa topologia, le uscite di guasto dello switch devono essere utilizzate solo se l'alimentazione relativa allo switch è stata progettata come ridondante; vedere *Switch Ethernet, pagina 55*.

Verificare che le impostazioni RSTP nelle unità di controllo della centrale, nel software FSP-5000-RPS e nello switch Ethernet corrispondano.

Modificare la priorità RSTP degli switch per il collegamento dei due loop poiché appartengono all'anello principale.

Il server OPC deve essere programmato separatamente

Programmare l'indirizzo IP, i nodi di rete, il gruppo di rete e l'RSN. Vedere la sezione corrispondente nel capitolo Installazione della Guida al collegamento in rete.

Il server OPC utilizza la porta 25000 standard.

Verificare che le impostazioni nel software di programmazione FSP-5000-RPS e nel server OPC corrispondano.

Parametri

- È possibile collegare il server OPC tramite un cavo Ethernet (in rame) o un cavo in fibra ottica.

In questi esempi, il loop a rappresenta l'anello principale. Il loop b è il loop secondario.

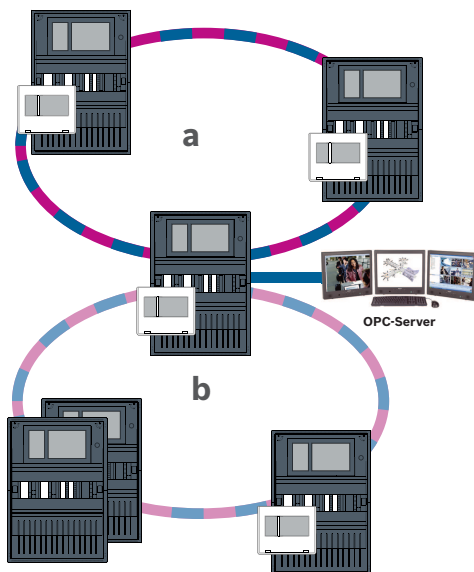


Figura 4.9: Collegamento del loop Ethernet tramite una centrale non ridondante

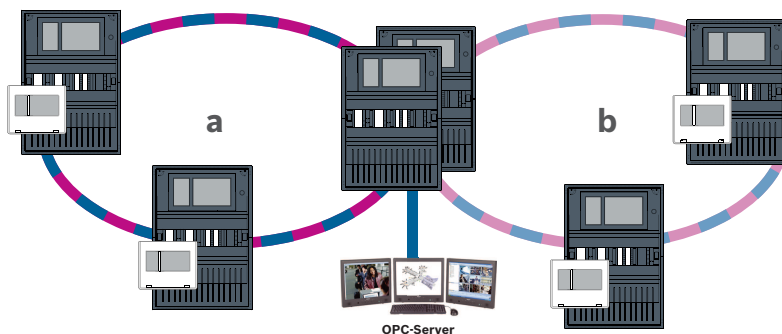


Figura 4.10: Collegamento del loop Ethernet tramite una centrale ridondante

5 Rete Ethernet

Nella rete, le connessioni Ethernet vengono monitorate costantemente. Se una connessione è stata interrotta, l'interruzione viene rilevata. Vengono rilevate anche le connessioni ripristinate. La diagnosi di rete della centrale mostra sempre l'indirizzo MAC degli host collegati attraverso la rete.

Indirizzi MAC

Per la connessione di rete, ogni unità di controllo della centrale fornisce gli indirizzi MAC riportati di seguito.

- Indirizzo MAC per l'host
- Indirizzo MAC per identificare la porta ETH1
- Indirizzo MAC per identificare la porta ETH2

A seconda del tipo di unità di controllo della centrale:

- Indirizzo MAC per identificare la porta ETH3
- Indirizzo MAC per identificare la porta ETH4

Regole per l'utilizzo di 4 porte Ethernet

Se la centrale dispone di 4 porte Ethernet, applicare le seguenti regole nell'ordine indicato. Bosch supporta solo le reti costruite in base alle seguenti regole.

1. Per il collegamento in rete delle centrali è necessario utilizzare ETH1 e ETH2. Uno switch RSTP esterno su ETH1 o ETH2 deve essere utilizzato unicamente per il collegamento in rete delle centrali.
2. Per collegare OPC, FSM-5000-FSI, Praesideo/PAVIRO o UGM-2040 è necessario utilizzare ETH3. È possibile collegare uno switch RSTP esterno, che non deve essere utilizzato per il collegamento in rete delle centrali.
3. Per Remote Services è necessario utilizzare ETH4. Se non è richiesto il collegamento a Remote Services, è possibile utilizzare ETH4 per collegare OPC, FSM-5000-FSI, Praesideo/PAVIRO o UGM-2040.
4. In assenza di un collegamento in rete delle centrali tramite ETH1 e ETH2, questi possono essere utilizzati individualmente per il collegamento di OPC, FSM-5000-FSI, Praesideo/PAVIRO o UGM-2040.

5.1 Protocolli

SNMP

Il protocollo SNMP consente di monitorare e controllare i componenti di rete. A tal fine, è possibile leggere o modificare i parametri dei nodi di rete. Per questo, sarà necessario il software appropriato per la gestione di rete (ad es. Hirschmann HiVision).



Avviso!

La rete utilizza la stringa comunità SNMP fissa: PUBLIC

Nota: la serie AVENAR panel non supporta ancora il protocollo SNMP.

LLDP

LLDP è un protocollo di base standardizzato IEEE che consente di condividere le informazioni di rete tra dispositivi adiacenti. Queste informazioni vengono

- fornite come parte dei dati SNMP e
- visualizzate tramite il display della centrale come parte dei dati diagnostici della rete.

RSTP

RSTP è un protocollo di rete standardizzato IEEE. RSTP garantisce che non siano presenti loop nelle reti. I percorsi ridondanti vengono rilevati nella rete, disattivati ed attivati quando necessario (errore di connessione).

Il protocollo viene utilizzato esattamente a tale scopo nella rete.

Una modifica della topologia a seguito di un errore di connessione viene annullata automaticamente una volta ripristinata.

5.2

Diametro della rete

Il diametro dell'anello delle reti di centrali Ethernet RSTP non deve essere maggiore di 32.



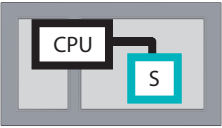
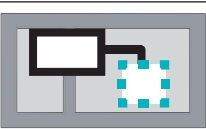
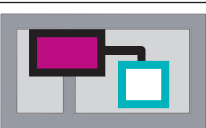
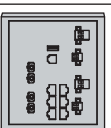
Definizione

Il diametro di una rete corrisponde al numero di switch RSTP sulla sezione più lunga possibile senza loop tra 2 endpoint qualsiasi della rete.

In relazione a una rete di centrali Ethernet RSTP, è necessario prendere in considerazione quanto segue:

- Ciascuna unità di controllo della centrale include un endpoint ed uno switch RSTP interno.
- Una combinazione di unità di controllo della centrale e unità di controllo della centrale ridondante viene considerata come un solo switch RSTP.
- I media converter non sono considerati switch RSTP.
- Le connessioni CAN BUS mantengono i limiti di 1 km tra una MPC e la successiva nel caso di connessione a loop.
- I server OPC non vengono considerati in relazione al diametro.

Chiave

	Processore centrale nell'unità di controllo della centrale oppure nel tastierino remoto.
	Switch RSTP interno all'unità di controllo della centrale o nel tastierino remoto.
	Unità di controllo della centrale o tastierino remoto con processore centrale e switch RSTP interno.
	Unità di controllo della centrale ridondante con processore centrale e switch RSTP interno.
	Unità di controllo della centrale o tastierino remoto Punto iniziale o endpoint per la determinazione del diametro della rete negli esempi.
	Switch Ethernet come switch RSTP esterno (in genere, Ethernet Switch MM)

2 centrali collegate formano il loop più piccolo possibile. Il diametro di questa rete è uguale a 2, poiché gli switch RSTP interni sono situati tra gli endpoint.

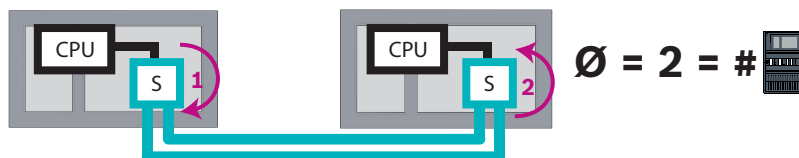


Figura 5.1: Diametro di rete di un loop con 2 centrali

In un loop di centrali senza switch RSTP esterni, il diametro della rete corrisponde al numero di centrali installate.

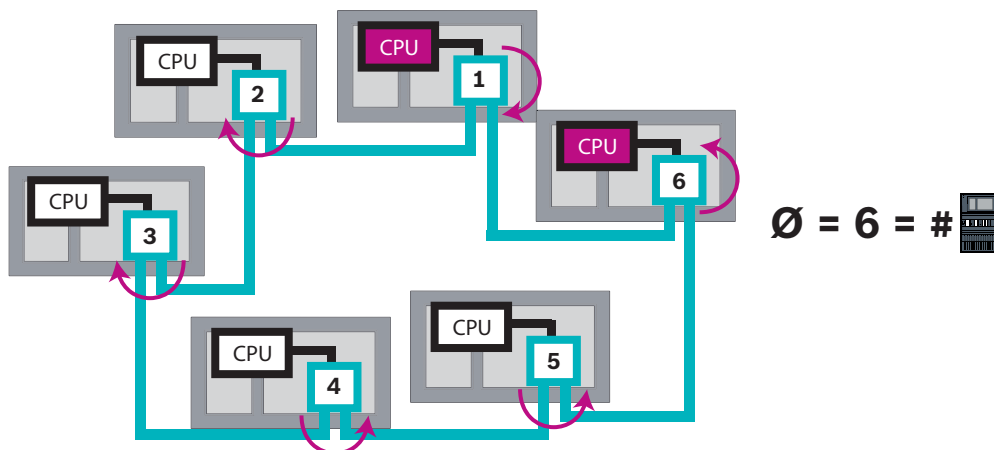


Figura 5.2: Diametro di rete di un loop con 6 centrali

Se anello principale e loop secondari sono collegati mediante switch Ethernet, è necessario prendere in considerazione gli switch RSTP esterni.

**Avviso!**

Lunghezza cavo TX

Tutte le connessioni IP devono essere dirette o tramite media converter approvati da Bosch. La lunghezza da nodo a nodo del cavo TX deve essere inferiore a 100 m.

**Avviso!**

VdS 2540

Per soddisfare i requisiti delle linee guida VdS 2540 per i percorsi di trasmissione dati, utilizzare un cavo in fibra ottica per le connessioni Ethernet. Per i collegamenti all'interno dell'alloggiamento è possibile utilizzare cavi Ethernet TX.

5.4

Creazione o modifica di una rete Ethernet

Sono disponibili diverse procedure per la creazione di una rete Ethernet di centrali di controllo allarme incendio. Le 2 procedure descritte di seguito si differenziano nelle dimensioni delle reti e nel numero di operazioni di installazione e configurazione eseguite parallelamente.

Regole per l'utilizzo di 4 porte Ethernet

Se la centrale dispone di 4 porte Ethernet, applicare le seguenti regole nell'ordine indicato. Bosch supporta solo le reti costruite in base alle seguenti regole.

1. Per il collegamento in rete delle centrali è necessario utilizzare ETH1 e ETH2. Uno switch RSTP esterno su ETH1 o ETH2 deve essere utilizzato unicamente per il collegamento in rete delle centrali.
2. Per collegare OPC, FSM-5000-FSI, Praesideo/PAVIRO o UGM-2040 è necessario utilizzare ETH3. È possibile collegare uno switch RSTP esterno, che non deve essere utilizzato per il collegamento in rete delle centrali.
3. Per Remote Services è necessario utilizzare ETH4. Se non è richiesto il collegamento a Remote Services, è possibile utilizzare ETH4 per collegare OPC, FSM-5000-FSI, Praesideo/PAVIRO o UGM-2040.
4. In assenza di un collegamento in rete delle centrali tramite ETH1 e ETH2, questi possono essere utilizzati individualmente per il collegamento di OPC, FSM-5000-FSI, Praesideo/PAVIRO o UGM-2040.

Creazione di una rete Ethernet (progetti più piccoli)

Questa procedura è adatta per i progetti di installazione del sistema di rivelazione incendio in cui interviene solo un numero limitato di tecnici contemporaneamente.

1. Progettare la rete.
2. Creare la rete in FSP-5000-RPS e configurare le relative impostazioni.
3. Stampare le informazioni sulla rete e custodirle oppure archivarle sul laptop.
4. Installare le centrali di controllo e i cavi di rete, quindi collegarle a una rete.
5. Configurare le impostazioni di rete per le singole centrali di controllo direttamente dal display attenendosi al materiale stampato.
6. Ripristinare ogni centrale di controllo nella rete per attivare la configurazione di rete.
7. Collegare il computer con il software di programmazione FSP-5000-RPS a una centrale di controllo nella rete. Caricare questa configurazione in tutte le altre centrali di controllo nella rete attraverso questa centrale. Le centrali ridondanti utilizzano la configurazione della centrale principale.
8. Eseguire un ripristino per ripristinare i messaggi di errore/guasto. Rettificare eventuali errori.

Configurare le impostazioni di rete prima sulle centrali di controllo. Ciò presenta il vantaggio di poter programmare le altre centrali di controllo nella rete da un'unica centrale di controllo.

Creazione di una rete Ethernet (progetti di medie e grandi dimensioni)

Questa procedura è adatta per i progetti che prevedono un numero di operazioni eseguite contemporaneamente da diversi team. Poiché molte operazioni eseguite durante l'installazione e la configurazione prevedono il riavvio della centrale di controllo allarme incendio, la rete non viene avviata in questa procedura se non in una fase successiva.

1. Progettare la rete.
2. Creare una configurazione della rete senza periferiche con FSP-5000-RPS.
3. Stampare le informazioni sulla rete e custodirle oppure archivarle sul laptop.
4. Installare i cavi di rete e controllare le singole sezioni o i singoli loop.
5. Installare le centrali e metterle in funzione come centrali autonome.
6. Installare le periferiche nelle centrali.
7. Configurare ogni centrale con FSP-5000-RPS.
8. Assicurarsi che le singole centrali funzionino correttamente.
9. Mettere in funzione i singoli loop della rete, uno dopo l'altro, a seconda della topologia. Iniziare con l'anello principale.
 - Creare una configurazione per l'anello principale in FSP-5000-RPS. Importare tutte le necessarie configurazioni delle centrali. Configurare le impostazioni di rete e stamparle.
 - Collegare tutte le centrali a una rete.
 - Configurare le impostazioni di rete per le singole centrali di controllo direttamente dal display della centrale attenendosi al materiale stampato.
 - Ripristinare ogni centrale di controllo per caricare la configurazione di rete.
 - Interrogare ("ping") le centrali adiacenti per controllare la comunicazione di rete.
 - Mettere in funzione l'intero anello di centrali e risolvere eventuali errori.Mettere in funzione i loop secondari sulla base dell'anello principale.

Aggiunta di una centrale a una rete

1. Modificare la configurazione di rete in FSP-5000-RPS.
2. Stampare le informazioni sulla rete e custodirle oppure archivarle sul laptop.
3. Installare la centrale di controllo e i cavi di rete, quindi collegarli alla rete.
4. Configurare le impostazioni di rete per le singole centrali di controllo direttamente dal display, attenendosi al materiale stampato.
5. Ripristinare la centrale e le centrali adiacenti per attivare la configurazione di rete.

Rimozione di una centrale dalla rete

1. Modificare la configurazione di rete in FSP-5000-RPS.
2. Stampare le informazioni sulla rete e custodirle oppure archivarle sul laptop.
3. Configurare le impostazioni di rete per le centrali di controllo adiacenti direttamente dal display, attenendosi al materiale stampato.
4. Disattivare la centrale e l'alimentazione (rete e batteria) prima di rimuoverla dalla rete.
5. Ripristinare le centrali adiacenti per attivare la configurazione di rete.

6 Rete CAN

Topologia loop

Nella topologia loop, il cavo CAN viene sempre instradato da un terminale CAN1 a un terminale CAN2 [CAN1 ⇒ CAN2]. La lunghezza del cavo dipende dalla sezione trasversale del cavo.

Collegamento CAN

Il collegamento CAN è una connessione a due conduttori (CAN-H e CAN-L). Collegare CAN-H a CAN-H e collegare CAN-L a CAN-L per una connessione a due conduttori. In casi eccezionali, ad esempio con una carica elettromagnetica elevata o una differenza notevole nel potenziale di messa a terra, potrebbe essere necessaria una connessione a tre conduttori (CAN-H, CAN-L

e CAN-GND). Collegare CAN-H a CAN-H, CAN-L a CAN-L e CAN-GND a CAN-GND per una connessione a tre conduttori. I fili schermati del cavo CAN sono collegati solo all'alloggiamento in metallo della centrale su un lato.

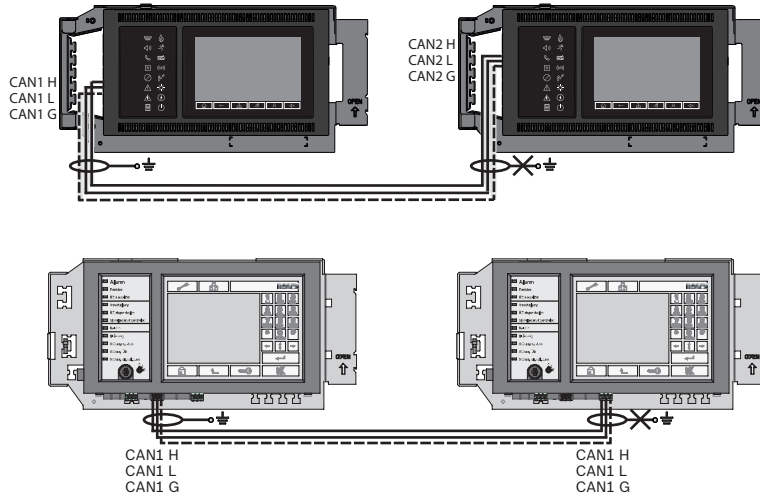


Figura 6.1: Connessione CAN (in alto: AVENAR, in basso: FPA)

Lunghezza del cavo per il collegamento in rete

La lunghezza massima del cavo consentita dipende dalla resistenza loop del cavo utilizzato e dal numero dei nodi di comunicazione.

Esempio: il cavo rosso del rivelatore incendio J-Y (St) Y 2 x 2 x 0,8 mm consente il collegamento di due nodi con distanza massima di circa 800 m.



Avviso!

È possibile determinare la distanza tra due nodi nella topologia loop leggendo il valore all'altezza dei due nodi nel diagramma.

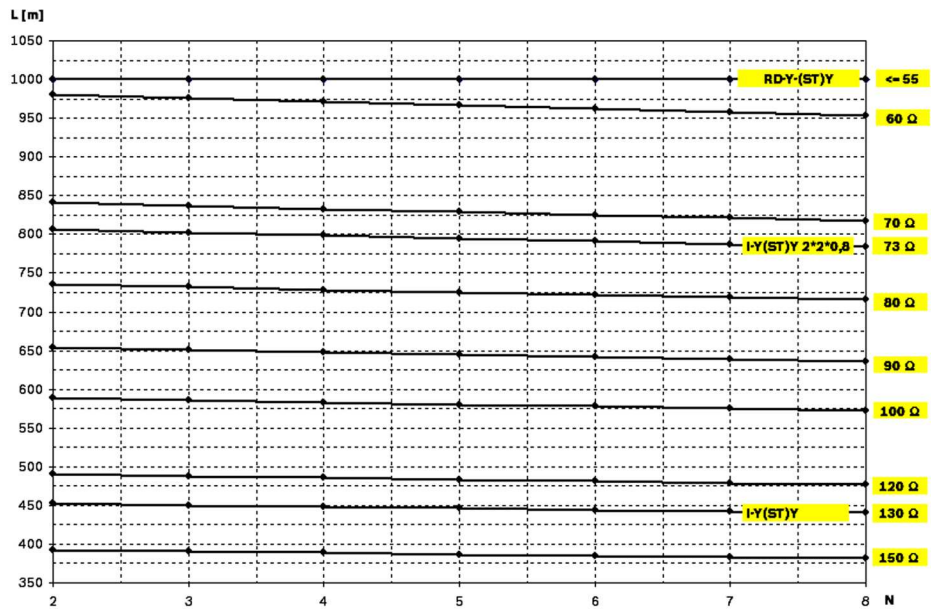


Figura 6.2: Rete CAN: lunghezza del cavo realizzabile, a seconda del numero di nodi e della resistenza del cavo

L = lunghezza cavo in metri

N = numero di nodi

6.1 Creazione o modifica di una rete CAN






Questa procedura è adatta per i progetti di installazione del sistema di rivelazione incendio in cui interviene solo un numero limitato di tecnici contemporaneamente.

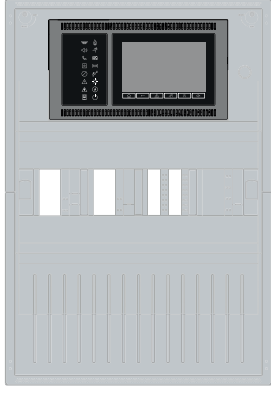
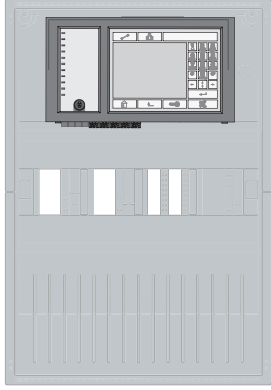
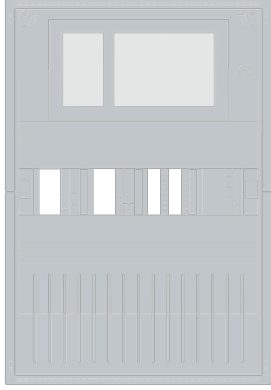
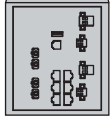



Procedura per la creazione di una rete CAN

1. Progettare la rete.
2. Creare la rete in FSP-5000-RPS.
3. Stampare le informazioni sulla rete e custodirle oppure archivarle sul laptop.
4. Installare le centrali di controllo e collegare a una rete con i cavi CAN.
5. Collegare il computer con il software di programmazione FSP-5000-RPS a una centrale di controllo nella rete. Caricare questa configurazione in tutte le altre centrali di controllo nella rete attraverso questa centrale. Le centrali ridondanti utilizzano la configurazione della centrale principale.
6. Eseguire un ripristino per ripristinare i messaggi di errore/guasto. Rettificare eventuali errori.

7 Modello di collegamento in rete Ethernet e CAN

Per creare reti di centrali corrispondenti alle topologie e ai servizi di connessione introdotti, è necessario attenersi al modello di collegamento in rete descritto in questo documento.

Icona	Descrizione
	Cavo Ethernet TX (in rame), lunghezza cavo TX da nodo a nodo < 100 m
	Cavo Ethernet FX (cavo in fibra ottica)
	Cavo Ethernet TX o FX, lunghezza cavo TX da nodo a nodo < 100 m
	Cavo CAN
	Alloggiamento Nota: per semplificare la panoramica dei vari modelli di collegamento in rete, le figure di questo capitolo mostrano sempre un piccolo alloggiamento della centrale per simboleggiare una centrale. Il piccolo alloggiamento della centrale non offre spazio sufficiente per montare gli switch, media converter e gateway illustrati in tutti i casi presentati. Utilizzare Safety Systems Designer per assicurarsi di ordinare alloggiamenti corretti per quantità e dimensioni per installare l'apparecchiatura.

Icona	Descrizione
	<p>AVENAR panel</p>
	<p>FPA</p>
	<p>AVENAR panel oppure FPA</p>
	<p>Switch Ethernet come switch RSTP esterno (in genere, switch Ethernet MM)</p>
	<p>Media converter</p>
	<p>Gateway di rete sicuro per Remote Services</p>
	<p>Connessione al server OPC, FSM-5000-FSI, Praesideo/PAVIRO o UGM-2040</p>

7.1 Rete di centrali su Ethernet

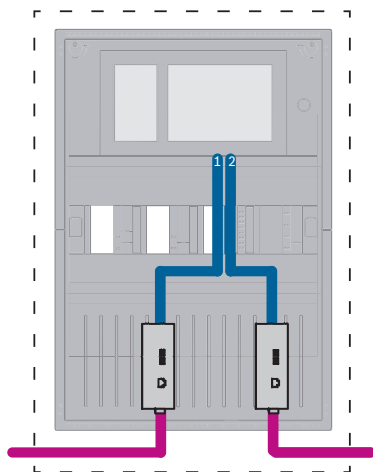


Figura 7.1: Rete di centrali su Ethernet

Per range maggiori di 100 m l'estensione con media converter è obbligatoria. Per range minori di 100 m i media converter potrebbero non essere necessari.

7.2 Rete di centrali su CAN

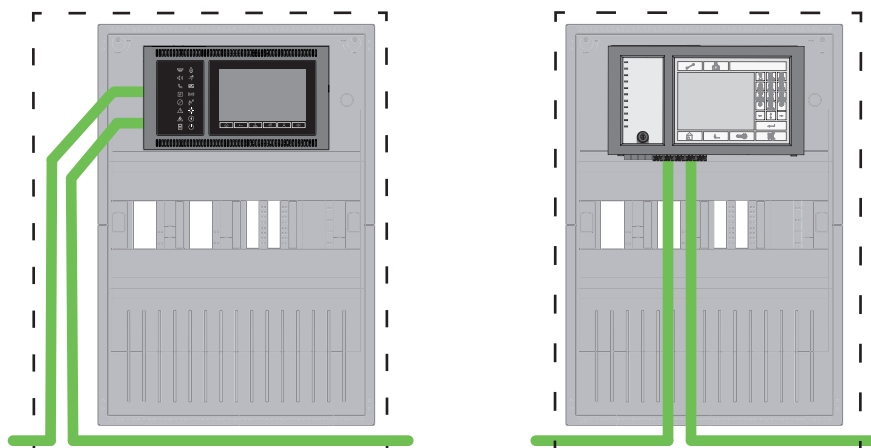


Figura 7.2: Rete di centrali su CAN

7.3 Connessione dei servizi alla centrale

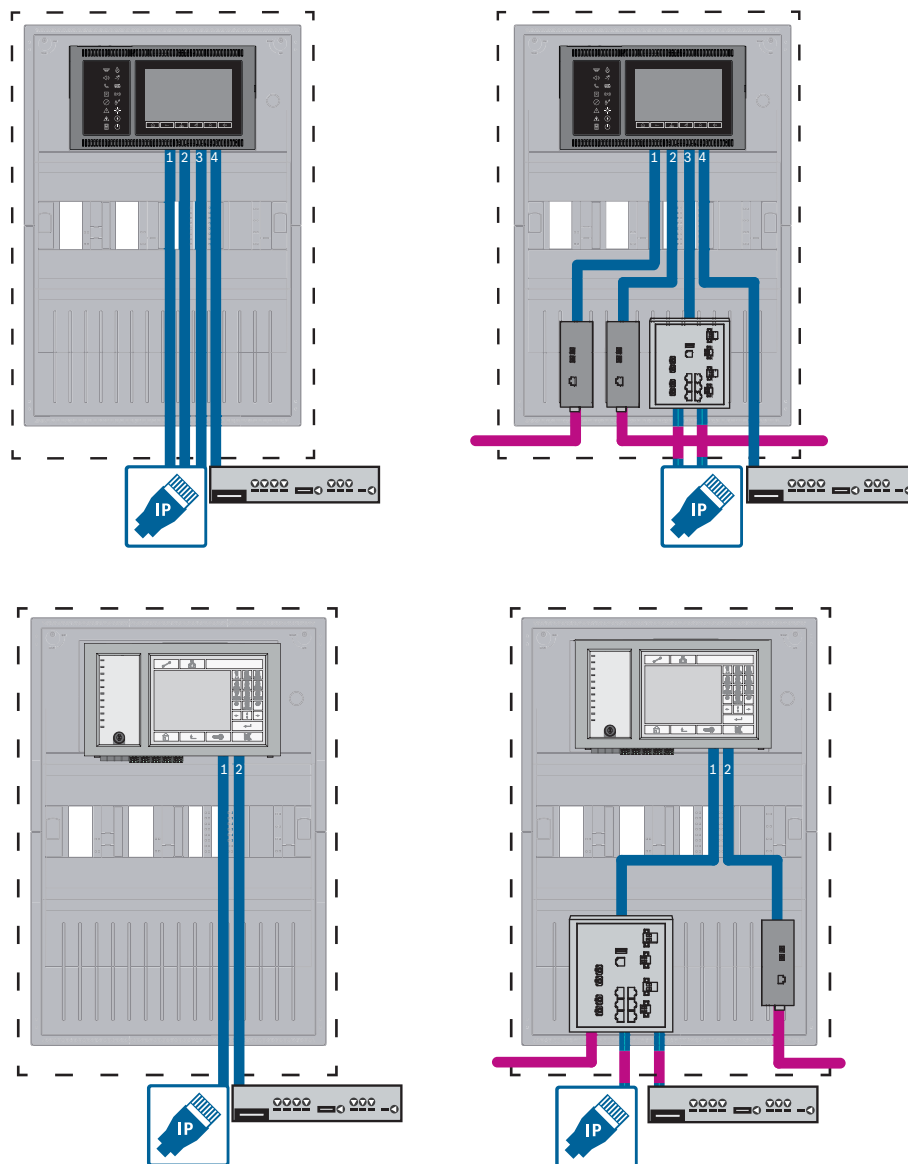


Figura 7.3: A sinistra: senza rete di centrali; a destra: con rete di centrali
 Per range maggiori di 100 m l'estensione con media converter è obbligatoria. Per range minori di 100 m i media converter potrebbero non essere necessari.

7.4 Rete di centrali su Ethernet con centrali ridondanti

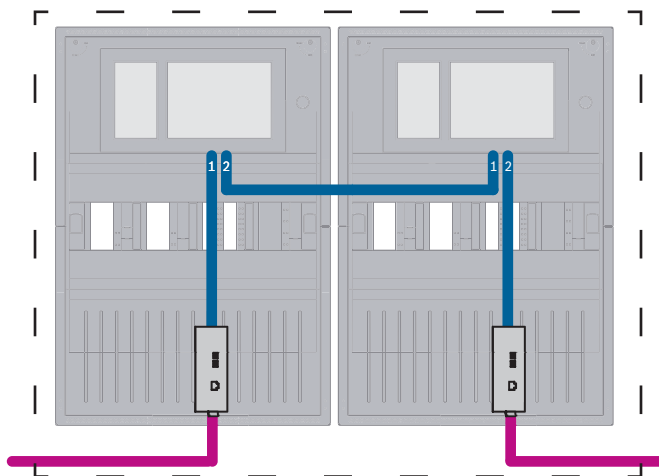


Figura 7.4: Rete di centrali su Ethernet con centrali ridondanti

Per range maggiori di 100 m l'estensione con media converter è obbligatoria. Per range minori di 100 m i media converter potrebbero non essere necessari.

7.5 Rete di centrali su CAN con centrali ridondanti

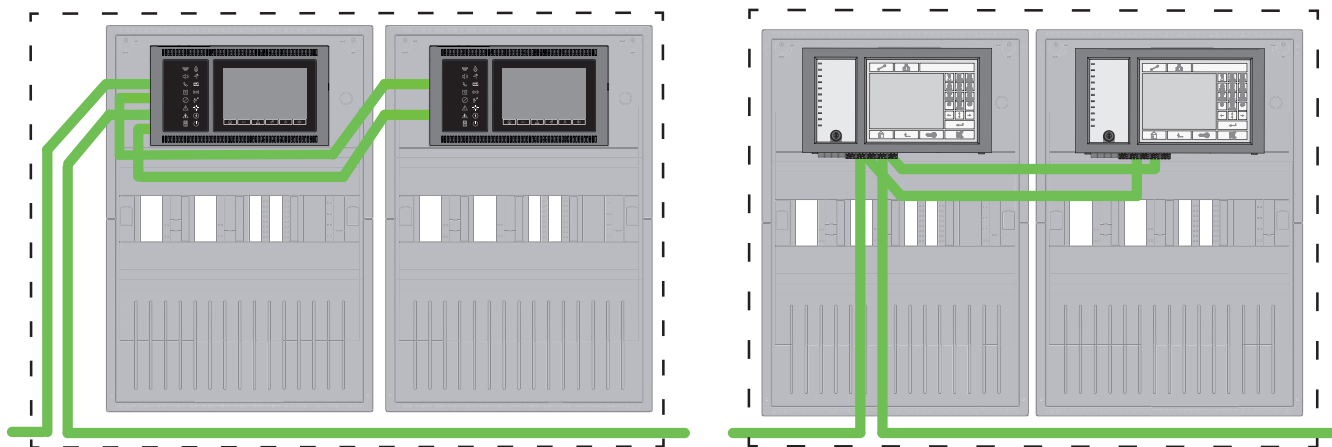


Figura 7.5: Rete di centrali su CAN con centrali ridondanti

7.6 Rete di centrali su due loop Ethernet

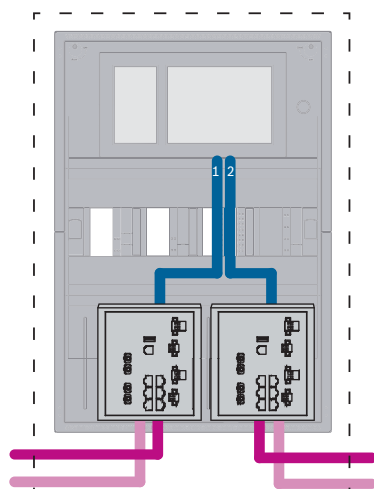


Figura 7.6: Connessione di reti Ethernet

7.7 Rete di centrali su due loop Ethernet con centrali ridondanti

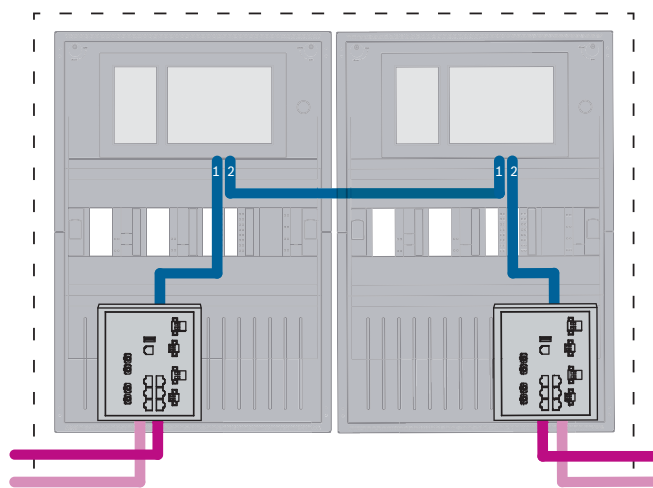


Figura 7.7: Connessione di reti Ethernet con centrali ridondanti

7.8 Connessione di reti Ethernet e CAN con centrali ridondanti

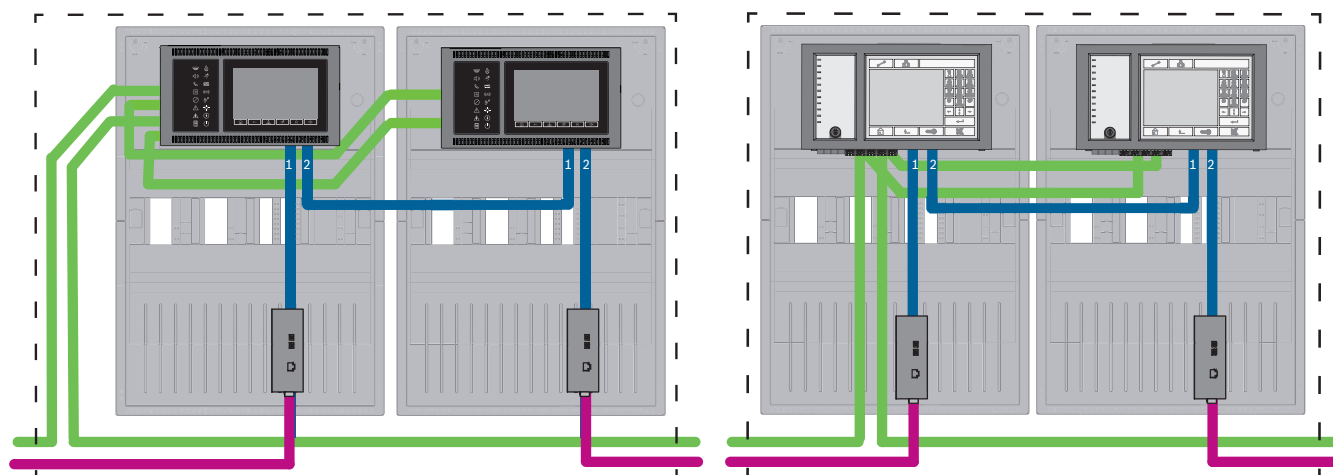


Figura 7.8: Connessione di reti Ethernet e CAN con centrali ridondanti

Per range maggiori di 100 m l'estensione con media converter è obbligatoria. Per range minori di 100 m i media converter potrebbero non essere necessari.

7.9 Connessione di servizi remoti a centrali ridondanti

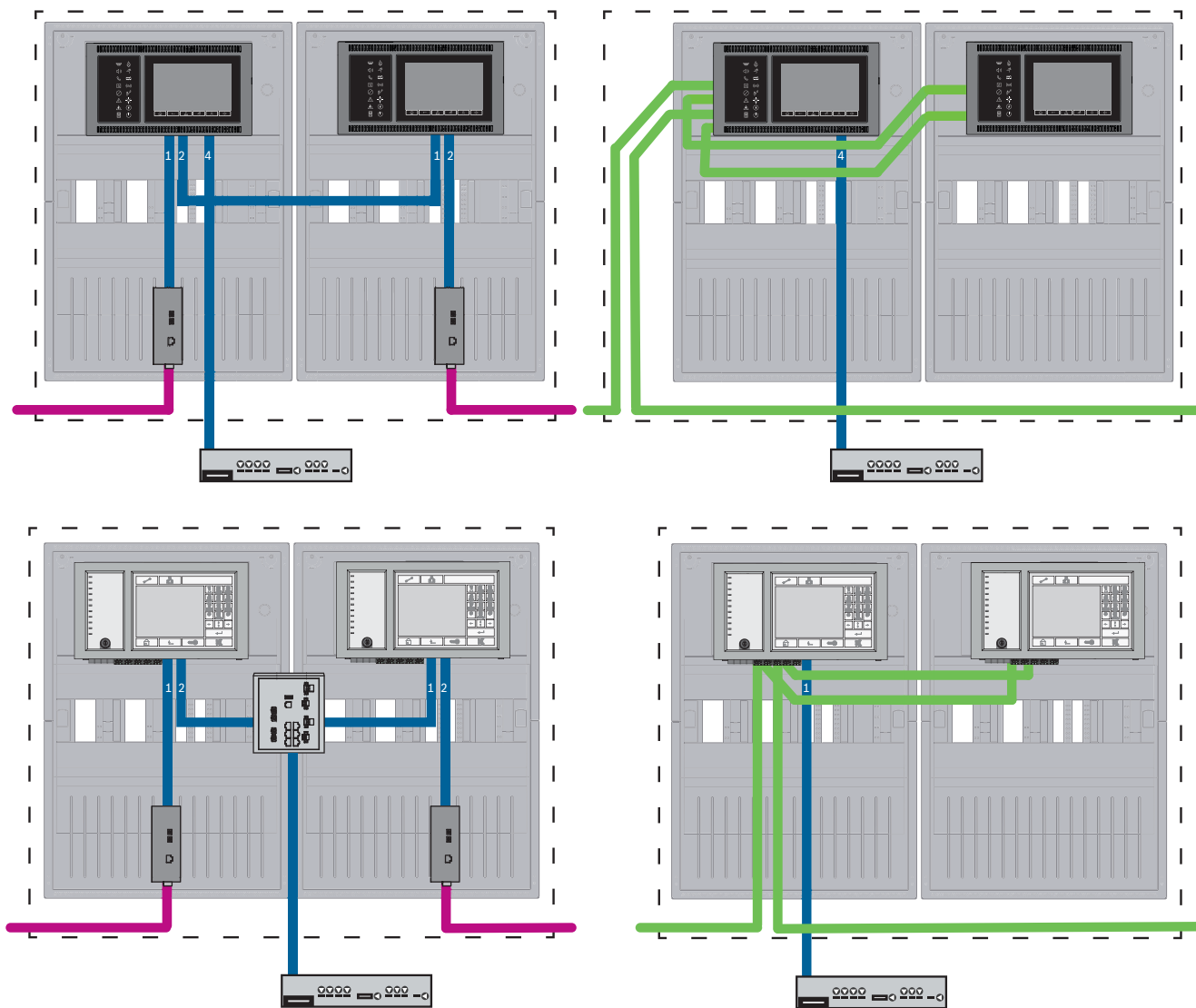


Figura 7.9: A sinistra: in rete Ethernet; a destra: in rete CAN

Per range maggiori di 100 m l'estensione con media converter è obbligatoria. Per range minori di 100 m i media converter potrebbero non essere necessari.

8 Remote Services

I seguenti servizi appartengono a Remote Services:

- Remote Connect
- Remote Alert
- Remote Maintenance

Il prerequisito per Remote Alert e Remote Maintenance è Remote Connect.

8.1 Remote Connect

Remote Connect fornisce una connessione a Internet affidabile e sicura, che consente l'accesso remoto a una centrale mediante FSP-5000-RPS. Remote Connect è la base di tutti i Remote Services. Per Remote Connect, utilizzare il gateway di rete sicuro.

Nel caso di una rete di centrali, una centrale della rete deve essere connessa a un gateway di rete sicuro. Esclusivamente questa connessione deve essere una connessione Ethernet dedicata.



Avviso!

Mentre Remote Connect supporta la connessione a una rete tramite Ethernet o CAN, le funzionalità Remote Alert e Remote Maintenance sono disponibili solo se il collegamento in rete tra le centrali viene fornito e configurato per il servizio.

Remote Connect deve essere abilitata nella configurazione FSP-5000-RPS di questa centrale. La seguente topologia mostra le unità di controllo della centrale connesse tramite Ethernet, dove un gateway di rete sicuro è collegato alla rete attraverso uno switch Ethernet (in genere, Ethernet Switch MM).

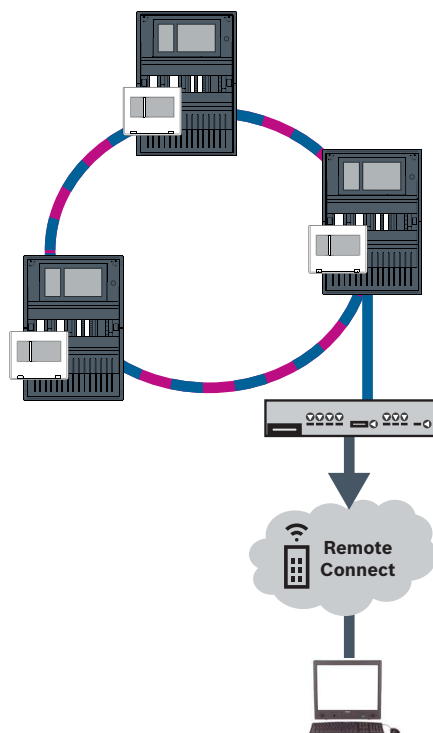


Figura 8.1: Remote Connect in un loop Ethernet



Avviso!

Per collegare le centrali tramite FX, utilizzare media converter approvati da Bosch.

Per impedire l'invio di traffico multicast EN 54-2 rilevante al router, utilizzare lo switch Ethernet (in genere, Ethernet Switch MM, BPA-ESWEX-RSR20) approvato con la versione 2.8 della centrale. Attivare lo snooping IGMP dello switch Ethernet; vedere la sezione corrispondente nel capitolo Installazione della Guida al collegamento in rete.

Avviso!

Il router Internet (o la rete aziendale che fornisce l'accesso a Internet) e il gateway di rete sicuro devono fornire sottoreti separate. Le centrali della rete di centrali non possono essere collocate nella sottorete del router Internet. Inoltre, non è possibile sovrapporre le sottoreti. Nel caso di sottoreti sovrapposte, è necessario separarle modificando gli indirizzi IP sul lato rete di centrali.

Inoltre, è necessario propagare le modifiche al gateway di rete sicuro. A tal fine, avviare l'interfaccia Web attraverso un browser Web:

- Indirizzo: <https://192.168.1.254>

- Nome utente: bosch

- Password: ipti83

In **Configuration** (Configurazione) -> **Network (LAN)** (Rete (LAN)) è possibile modificare l'indirizzo IP. L'indirizzo del **Gateway predefinito**: nella configurazione dell'unità di controllo della centrale deve corrispondere all'indirizzo IP del gateway di rete sicuro.



Avviso!

In conformità alle linee guida DIBt, il ripristino da remoto tramite Remote Services non è consentito per ripristinare l'operatività dei sistemi di controllo delle porte con apertura motorizzata.



La seguente topologia mostra una rete CAN in cui un gateway di rete sicuro è collegato alla rete attraverso una porta Ethernet.

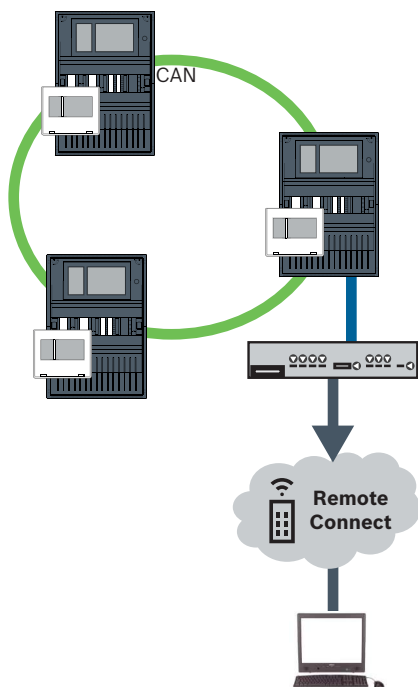


Figura 8.2: Remote Connect in un loop CAN

8.2

Remote Alert

Mediante Remote Alert, una centrale invia le relative informazioni sullo stato a Remote Portal.

I dati trasferiti vengono analizzati con Remote Alert. In caso di un evento imprevisto, l'utente viene informato sugli avvisi ricevuti con una notifica tramite SMS e/o e-mail. Remote Alert è inoltre disponibile per Private Secure Network.

8.3 Remote Maintenance

Remote Maintenance offre la possibilità di monitorare in remoto alcuni parametri di vari elementi di sicurezza connessi ad una centrale antincendio. Tramite il Remote Portal è possibile eseguire il walktest.

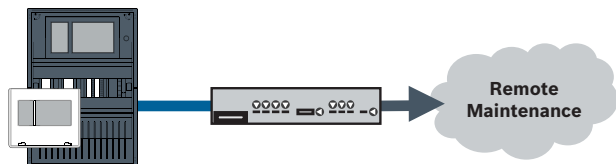


Figura 8.3: Remote Maintenance



Avviso!

Le connessioni Ethernet utilizzate esclusivamente per il trasferimento dei dati di Remote Maintenance possono essere realizzate come cavi in fibra ottica o cavi Ethernet. Si notino le lunghezze massime consentite dei cavi.



Avviso!

Per collegare le centrali tramite FX, utilizzare media converter approvati da Bosch.

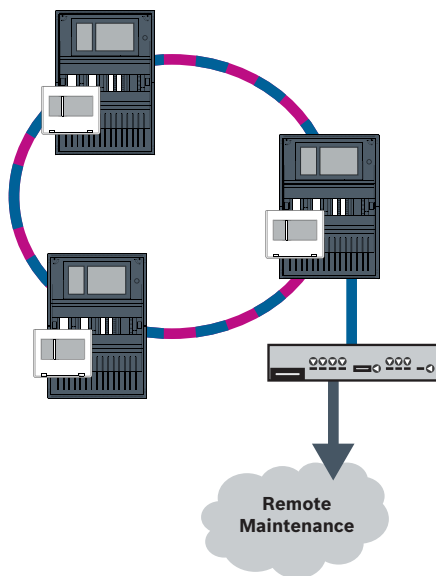


Figura 8.4: Remote Maintenance

Quando si utilizza Remote Maintenance con reti Ethernet, è necessario collegare una centrale della rete al router per la trasmissione dati. Tutti i dati raccolti vengono trasferiti dalla rete tramite questo collegamento.

Remote Maintenance per Remote Portal

Remote Maintenance raccoglie i dati dei moduli funzionali e dei dispositivi LSN pertinenti e li invia al Remote Portal, dove vengono analizzati e visualizzati per le attività di manutenzione.

Remote Maintenance per rete privata protetta

Remote Maintenance può essere configurato per Private Secure Network: i dati raccolti vengono inviati a un sistema CMS (server di gestione centrale).



Attenzione!

Remote Services richiede una connessione IP protetta. È necessario utilizzare Bosch Remote Services o una connessione con Private Secure Network.

Private Secure Network viene fornito con una rete IP basata su DSL, con accesso wireless opzionale sul lato della centrale (EffiLink). Remote Services per Private Secure Network è disponibile solo in Germania con un contratto di assistenza con Bosch BT-IE.



Avviso!

Per collegare le centrali tramite FX, utilizzare media converter approvati da Bosch.

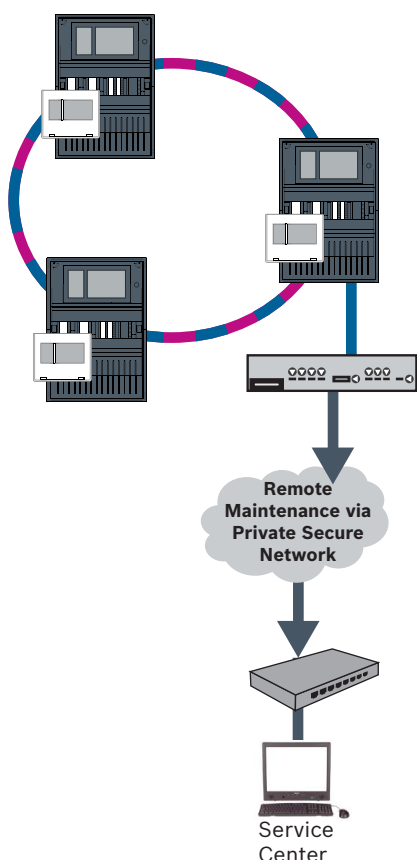


Figura 8.5: Remote Maintenance per rete privata protetta

Per Remote Maintenance, è necessario immettere l'indirizzo IP del server e la porta del server del sistema Remote Maintenance nel software di programmazione FSP-5000-RPS. Assegnare un ID di rete della centrale univoco alla rete.

Lo switch per il collegamento del CMS deve essere programmato separatamente

Per programmare le impostazioni di ridondanza ed indirizzo IP dello switch, vedere *Impostazioni dello switch, pagina 44*. Quando lo switch viene installato nelle immediate vicinanze (senza barriere intermedie), l'alimentazione non deve essere progettata come ridondante e le uscite di guasto non vengono pertanto utilizzate.

Verificare che le impostazioni RSTP nelle unità di controllo della centrale, nel software FSP-5000-RPS e nello switch Ethernet corrispondano.

8.4 Remote Portal

Requisiti



Avviso!

Per evitare le operazioni di riconfigurazione o regolazione se si utilizzano Remote Services, assicurarsi che siano soddisfatti i seguenti requisiti:

- centrale con firmware 2.19.7 o superiore, tutte le centrali collegate tramite Ethernet, interfacce Ethernet abilitate e impostazioni Ethernet standard
- Remote Connect abilitato nella configurazione della centrale con FSP-5000-RPS
- gateway di rete sicuro per Remote Services disponibile
- computer con FSP-5000-RPS 4.8 o versione successiva installato e accesso a Internet



Avviso!

Evitare l'aggiornamento del gateway di rete sicuro durante la connessione.

Gli aggiornamenti del gateway di rete sicuro vengono eseguiti regolarmente nelle prime ore del mattino. Specificare pertanto il fuso orario in **System** (Sistema) -> **General Settings** (Impostazioni generali) -> **Timezone** (Fuso orario).

Istruzioni

Per utilizzare Remote Services è necessario essere utenti di un account Remote Portal.

Fase 1: Creazione di un account Remote Portal

È possibile impostare più utenti per un unico account Remote Portal. Ogni account Remote Portal ha un Remote ID univoco, che rappresenta una sola società. Se non è possibile utilizzare un account Remote Portal esistente, è necessario crearne uno:

1. In <https://remote.boschsecurity.com> -> **Sign Up** (Iscrizione) inserire il nome, la società, l'indirizzo e-mail e creare una password. Leggere le condizioni generali e selezionare **I agree to the terms and conditions** (Accetto le condizioni generali). Leggere l'informativa sulla privacy e selezionare **I agree to the privacy statement** (Accetto l'informativa sulla privacy).
2. Fare clic su **Register** (Registra).
Il Remote Portal invia un'e-mail all'indirizzo specificato contenente un collegamento di attivazione.
3. Per attivare l'account, fare clic sul collegamento di attivazione. Su Remote Portal, fare clic sul nome utente e selezionare **Account Settings** (Impostazioni account). Viene visualizzato l'Remote ID. Questo Remote ID sarà necessario sull'unità di controllo della centrale in un secondo momento.

Per fornire a ciascuno dei tecnici un proprio account, è possibile creare diversi utenti per lo stesso Remote ID:

L'accesso a Remote Portal è stato effettuato.

- ▶ Selezionare **Users** (Utenti) -> **New Technician** (Nuovo tecnico). Inserire quindi i dati richiesti e confermare facendo clic su **Save** (Salva).

Fase 2: Connessione del gateway di rete sicuro

Per stabilire Remote Services, utilizzare un gateway di rete sicuro.

1. Connettere la porta WAN del gateway di rete sicuro al router Internet o alla rete aziendale che fornisce l'accesso a Internet.
2. Verificare qui la disponibilità dei seguenti protocolli e porte per il gateway di rete sicuro (necessaria per la connessione a Remote Services).

Protocollo	Porta predefinita	Descrizione
HTTP	80 e 8080	Per la registrazione di Remote Connect e per Remote Maintenance
VPN IPsec	UDP 500 e UDP 4500	Per Remote Connect

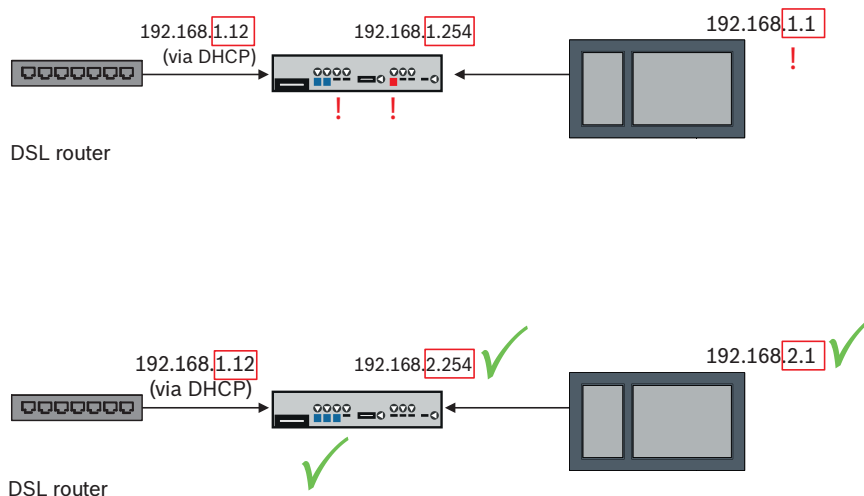
3. Connettere la porta LAN1 del gateway di rete sicuro alla porta Ethernet designata dell'unità di controllo della centrale utilizzando il cavo di rete CAT5 RJ45 in dotazione. Osservare le topologie possibili.
4. Collegare il gateway di rete sicuro a un'alimentazione di rete da 100 V - 230 V utilizzando l'alimentazione in dotazione.

LED WAN acceso (blu), quando la connessione a Internet è stata stabilita. LED VPN acceso (blu) immediatamente dopo, a indicare che è stata stabilita una connessione VPN al Remote Portal.

Ciascuna centrale collegata o una rete di centrali dispone di un System ID univoco.

Separazione delle sottoreti (LED VPN spento)

In presenza di sottoreti sovrapposte, il collegamento del gateway di rete sicuro per Remote Services non riesce (LED VPN spento). Nell'esempio seguente viene illustrato un gateway di rete sicuro e un'unità di controllo della centrale nello stesso range indirizzi del router DSL.



Un gateway di rete sicuro rileva sottoreti sovrapposte senza generare ambiguità: il LED di Alarm lampeggia costantemente.

La separazione delle sottoreti viene eseguita modificando il terzo ottetto dell'indirizzo IP. Modificare gli indirizzi IP sul lato della rete di centrali. Una volta modificato l'indirizzo IP, è necessario propagare le modifiche al gateway di rete sicuro. A tal fine, avviare l'interfaccia Web attraverso un browser Web:

- Indirizzo: <https://192.168.1.254>
- Nome utente: bosch
- Password: ipti83

In **Configuration** (Configurazione) -> **Network (LAN)** (Rete (LAN)) è possibile modificare l'indirizzo IP. L'indirizzo del **Gateway predefinito**: nella configurazione dell'unità di controllo della centrale deve corrispondere all'indirizzo IP del gateway di rete sicuro.

Fase 3: Creazione di una connessione remota

1. Sulla centrale, utilizzare le impostazioni Ethernet standard.
2. Riavviare la centrale.
3. Per l'autenticazione, selezionare **Configuration** (Configurazione) -> **Network Services** (Servizi di rete) -> **Change date / time** (Modifica data/ora), inserire la data attuale e confermare le impostazioni.
4. Selezionare **Configuration** (Configurazione) -> **Network Services** (Servizi di rete) -> **Remote Services**, quindi inserire l'Remote ID.

È possibile verificare lo stato della connessione remota: selezionare **Diagnostics** (Diagnostica) -> **Network Services** (Servizi di rete) -> **Remote Services** sull'unità di controllo della centrale.

Fase 4: Assegnazione di una licenza in Remote Portal

Per attivare l'utilizzo dei Remote Services è necessario assegnare una licenza in Remote Portal. Una licenza viene fornita automaticamente all'account alla prima connessione.

**Avviso!**

Non è possibile riassegnare una licenza già assegnata o sospesa.

1. In <https://remote.boschsecurity.com> -> **Login** (Accesso) inserire l'indirizzo e-mail e la password.
2. Selezionare **Systems** (Sistemi).
3. Selezionare il sistema.
4. In **Services** (Servizi) fare clic sul pulsante **Add Service** (Aggiungi servizio) sotto il servizio.
5. Per impostazione predefinita la licenza verrà automaticamente rinnovata: **Service Settings** (Impostazioni assistenza), opzione **With Auto-Renew** (Con rinnovo automatico).
6. Fare clic su **Save** (Salva) per confermare le impostazioni.

Dopo aver assegnato la licenza è possibile utilizzare il servizio corrispondente. Una licenza assegnata viene visualizzata con un segno verde.

Fase 5: riordinare la licenza

1. Ordinare licenze valide un anno dai sistemi di rivelazione incendio Bosch. Ciascuna rete richiede una propria licenza.
Bosch invia un'e-mail all'indirizzo specificato. L'e-mail include numeri di registrazione della licenza univoci per la quantità di licenze ordinate, nonché istruzioni e un collegamento a Remote Portal.
2. In <https://remote.boschsecurity.com> -> **Login** (Accesso) inserire l'indirizzo e-mail e la password.
3. Selezionare **Licenses** (Licenze).
4. Fare clic sul pulsante **+**.
5. Attenersi alle istruzioni riportate nella finestra **Add Licenses** (Aggiungi licenze) e confermare tramite **Save** (Salva).
6. L'elenco delle licenze viene aggiornato.

9**Sistemi di allarme vocale**

La seguente topologia mostra le unità di controllo della centrale collegate tramite Ethernet dove il sistema Praesideo/PAVIRO viene integrato nel loop di centrali mediante un'interfaccia Ethernet.

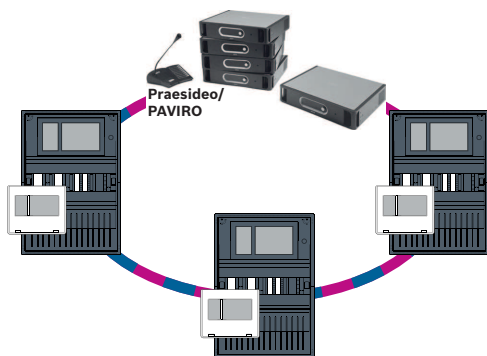


Figura 9.1: Loop Ethernet con Praesideo/PAVIRO

Utilizzare lo Ethernet Switch (in generale MM BPA-ESWEX-RSR20) approvato con versione firmware della centrale 2.8.

Per impedire l'invio di traffico multicast EN 54-2 rilevante al sistema Praesideo/PAVIRO, attivare lo snooping IGMP dell'MM; vedere la sezione corrispondente nel capitolo Installazione della Guida al collegamento in rete.

In ogni unità di controllo della centrale di una rete CAN è possibile collegare un sistema Praesideo/PAVIRO utilizzando un'interfaccia Ethernet. La seguente topologia mostra le unità di controllo della centrale collegate tramite CAN dove il sistema Praesideo/PAVIRO viene collegato a un'unità di controllo della centrale tramite un'interfaccia Ethernet.

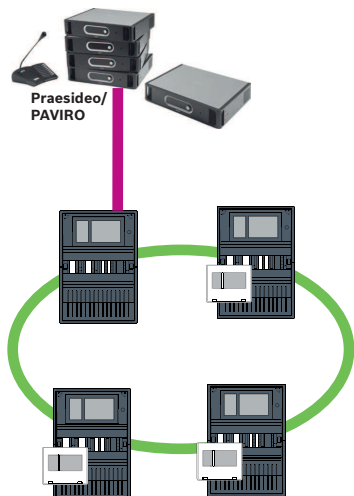


Figura 9.2: Collegamento di Praesideo/PAVIRO a una rete CAN



Avviso!

Poiché il traffico di rete CAN non verrà trasferito tramite connessione Ethernet, è necessario disattivare il collegamento in rete su IP nel software di programmazione FSP-5000-RPS. Se non viene disattivato, la rete non risulterà conforme allo standard EN 54.



Avviso!

Se è necessario utilizzare un'unità di controllo della centrale MPC-xxxx-B per il collegamento diretto a un sistema Praesideo/PAVIRO, procurarsi un cavo patch di cross-over poiché né Praesideo/PAVIRO né MPC-xxxx-B supportano Auto-MDI(X).

10

Installazione

Lista di controllo

Prima di procedere all'installazione della rete di centrali, esaminare tutti i punti definiti di seguito.

- Ethernet e CAN
 - La lunghezza massima delle linee dei cavi Ethernet TX, Ethernet FX, CAN TX e CAN FX è inferiore alla lunghezza massima di questi ultimi.
 - Tutte le periferiche ed il relativo cablaggio nelle singole centrali sono pianificati.
- Progettazione della rete
 - Tutti gli indirizzi IP e le impostazioni di rete per le singole centrali ed i componenti di rete aggiuntivi sono pianificati e disponibili.
 - È disponibile una panoramica dei componenti aggiuntivi da installare, ad esempio switch Ethernet e media converter, e del relativo cablaggio con le centrali vicine.
 - È disponibile una panoramica della topologia di rete da installare.
 - Tutte le impostazioni di ridondanza della rete sono pianificate e disponibili.

10.1 Impostazioni del media converter

Per utilizzare il media converter, sono richiesti solo alcuni passaggi:

- Impostare gli interruttori DIP.
- Collegare il convertitore di supporti ai cavi di rete FX e CAT5e.
- Alimentare il media converter attraverso il modulo di controllo batterie BCM interno.



Avviso!

I media converter sono alimentati solo attraverso il terminale di alimentazione 1. Il LED di errore sul media converter è pertanto costantemente acceso, senza, tuttavia, interferire sulla funzionalità del dispositivo.



Avviso!

Per il collegamento in rete, utilizzare solo i seguenti cavi:

Cavo Ethernet

Cavo patch Ethernet, schermato, CAT5e o superiore.

Si noti il raggio di curvatura minimo specificato nella sezione relativa al cavo.

Cavo in fibra ottica

Modalità multimodale: cavo patch Ethernet in fibra ottica, duplex I-VH2G 50/125 μ o duplex I-VH2G 62,5/125 μ , presa SC.

Modalità monomodale: cavo patch Ethernet in fibra ottica, duplex I-VH2E 9/125 μ .

Si noti il raggio di curvatura minimo specificato nella sezione relativa al cavo.



Avviso!

Consultare le guide all'installazione relative ai kit di montaggio per informazioni su come installare un media converter nell'alloggiamento di una centrale: FPM 5000 KMC(F.01U.266.845)FPM-5000-KES(F.01U.266.844)



Avviso!

La lunghezza massima di fibra ottica per i media converter multimodali è 2000 m.

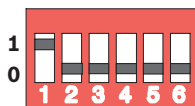
La lunghezza massima di fibra ottica per i media converter monomodali è 40 km.

Utilizzando gli interruttori DIP, configurare il media converter come mostrato nella figura riportata di seguito.



Avviso!

Modificare le impostazioni degli interruttori DIP sui media converter solo quando vengono disalimentati.



Numero interruttore DIP	Impostazione
1	Link Fault Pass-Through attivato
2	Ethernet: modalità automatica
3	Ethernet: 100 MBit
4	Ethernet: full duplex
5	Cavo in fibra ottica: full duplex
6	Collegamento non disponibile: disattivato

10.2 Installazione dello switch Ethernet



Avvertenza!

Luce laser

Non guardare in direzione del fascio ad occhio nudo o con strumenti visivi di qualunque tipo (ad es. lente di ingrandimento, microscopio). L'inosservanza di questo avviso costituisce un pericolo per gli occhi a una distanza inferiore a 100 mm. La luce emerge all'altezza dei terminali video o all'estremità dei cavi in fibra ottica ad essi collegati. Diodo laser CLASSE 2M, lunghezza d'onda 650 nm, uscita < 2 mW, in conformità alla normativa IEC 60825-1.



Avviso!

Fare riferimento alla guida all'installazione per il kit di montaggio per switch Ethernet FPM-5000-KES (F.01U.260.523).

10.3 Impostazioni dello switch

Per poter utilizzare gli switch nella rete, è necessario programmarli.

Collegare il laptop alla rete ed utilizzare il software HiDiscovery fornito dal produttore per eseguire la programmazione iniziale degli switch. Con questo software, eseguire la ricerca degli switch nella rete. Fare doppio clic su uno switch per selezionarlo ed assegnargli un indirizzo IP.

In seguito alla programmazione iniziale dell'indirizzo IP, è possibile utilizzare un browser web per richiamare l'interfaccia utente di configurazione relativa allo switch.



Avviso!

Consultare la guida utente del produttore per una descrizione precisa dell'installazione e della configurazione degli switch. Dati di accesso:

Utente: admin

Password: private

Utilizzare un browser per richiamare l'interfaccia utente di configurazione relativa agli switch. È necessario effettuare le seguenti impostazioni nello switch:

- Assegnare l'indirizzo IP, pagina 45,
- Programmare le impostazioni di ridondanza, pagina 45.

Inoltre, impostazioni opzionali quali:

- Programmazione del relè di guasto, pagina 46,
- Programmazione del monitoraggio dei collegamenti, pagina 47,

- *Attivazione dello snooping IGMP, pagina 47.*

10.3.1 Assegnare l'indirizzo IP

**Avviso!**

Suggerimento pratico:

Nella parte relativa al dispositivo dell'indirizzo IP, utilizzare numeri maggiori di 200 (xxx.xxx.xxx.200) per gli switch, se la configurazione di rete lo consente. Ciò permette una separazione più netta dall'identificatore host di un indirizzo IP.

Esempio:

Lo switch 192.168.1.201 è assegnato alla centrale con indirizzo IP 192.168.1.1.

**Avviso!**

Consultare i seguenti documenti del produttore per una descrizione precisa dell'installazione e della configurazione degli switch:

Guida utente all'installazione

Guida di riferimento per l'interfaccia basata su web

Utilizzare un browser per accedere all'interfaccia utente di configurazione relativa agli switch. Nel menu **Basic Settings -> Network** (Impostazioni di base -> Rete), impostare i valori seguenti a seconda della topologia scelta:

- Modalità: locale
- Indirizzo IP: l'indirizzo IP richiesto, ad es. 192.168.1.201
- Subnet mask: la subnet mask richiesta, ad es. 255.255.255.0
- Gateway: il gateway richiesto, ad es. 192.168.1.254 o 0.0.0.0 se non è richiesto alcun gateway

Fare clic su **Write** (Scrivi).

**Avviso!**

Le impostazioni delle singole voci di menu nella configurazione degli interruttori diventeranno effettive dopo aver fatto clic su **Write** (Scrivi).

Le impostazioni vengono salvate solo in maniera permanente, in modo che vengano conservate anche in seguito al riavvio del dispositivo, se in **Basic Settings -> Load/Save** (Impostazioni di base -> Carica/Salva) nel campo **Save** (Salva), si seleziona la voce **On the device** (Sul dispositivo) e si fa clic sul pulsante **Save** (Salva).

10.3.2 Programmare le impostazioni di ridondanza

Poiché le reti di centrali FPA utilizzano RSTP come protocollo di ridondanza, è necessario attivare e programmare il protocollo nell'interfaccia utente di configurazione:

Nel menu **Redundancy -> Spanning Tree -> Global** (Ridondanza -> Albero di spanning -> Globale), impostare i valori seguenti:

- Funzione: attivata
- Versione protocollo: RSTP
- Configurazione protocollo: utilizzare le stesse impostazioni configurate per le unità di controllo della centrale.

Fare clic su **Write** (Scrivi).

**Avviso!**

Le impostazioni delle singole voci di menu nella configurazione degli interruttori diventeranno effettive dopo aver fatto clic su **Write** (Scrivi).

Le impostazioni vengono salvate solo in maniera permanente, in modo che vengano conservate anche in seguito al riavvio del dispositivo, se in **Basic Settings -> Load/Save** (Impostazioni di base -> Carica/Salva) nel campo **Save** (Salva), si seleziona la voce **On the device** (Sul dispositivo) e si fa clic sul pulsante **Save** (Salva).

10.3.3**Programmazione del relè di guasto****Avviso!**

Il relè di guasto deve essere programmato per applicazioni che soddisfano almeno uno dei seguenti requisiti:

Esiste un collegamento tra due switch. Ciò è possibile in caso di anello principale con loop secondari, ed esempio.

L'alimentazione dello switch è progettata come ridondante.

**Avviso!**

Consultare i seguenti documenti del produttore per una descrizione precisa dell'installazione e della configurazione degli switch:

Guida utente all'installazione

Guida di riferimento per l'interfaccia basata su web

Utilizzare un browser per accedere all'interfaccia utente di configurazione relativa agli switch. In **Diagnosis -> Signal Contact** (Diagnosi -> Contatto di segnale) nella scheda **Signal Contact 1** (Contatto di segnale 1), impostare **Signal Contact Mode** (Modalità di contatto segnale) su **Device Status** (Stato dispositivo).

In **Diagnosis -> Device Status** (Diagnosi -> Stato dispositivo) nel campo **Monitoring** (Monitoraggio), impostare i valori seguenti:

- **Power Supply 1** (Alimentazione 1): **Monitor**
- **Connection Error** (Errore di connessione): **Monitor**

Tutte le altre opzioni devono essere impostate su **Ignore** (Ignora).

**Avviso!**

Le impostazioni di **Device Status** (Stato dispositivi) si applicano anche al LED di guasto dello switch.

Fare clic su **Write** (Scrivi).

**Avviso!**

Le impostazioni delle singole voci di menu nella configurazione degli switch diventeranno effettive dopo aver fatto clic su **Write** (Scrivi).

Le impostazioni vengono salvate solo in maniera permanente, in modo che vengano conservate anche in seguito al riavvio del dispositivo, se in **Basic Settings -> Load/Save** (Impostazioni di base -> Carica/Salva) nel campo **Save** (Salva), si seleziona la voce **On the device** (Sul dispositivo) e si fa clic sul pulsante **Save** (Salva).

10.3.4 Programmazione del monitoraggio dei collegamenti

**Avviso!**

L'impostazione per il monitoraggio dei collegamenti è necessaria solo se si utilizza il relè di guasto dello switch.

Se si desidera utilizzare il relè di guasto per il monitoraggio dei collegamenti dell'interruttore, è necessario specificare le porte da monitorare nella configurazione dello switch.

Attivare la casella di controllo **Forward Connection Error** (Inoltra errore di connessione) per le singole porte nel menu **Basic Settings -> Port Configuration** (Impostazioni base -> Configurazione porte).

Vengono monitorati solo i collegamenti per cui è stato attivato **Forward Connection Errors** (Inoltra errori di connessione).

Fare clic su **Write** (Scrivi).

**Avviso!**

Le impostazioni delle singole voci di menu nella configurazione degli switch diventeranno effettive dopo aver fatto clic su **Write** (Scrivi).

Le impostazioni vengono salvate solo in maniera permanente, in modo che vengano conservate anche in seguito al riavvio del dispositivo, se in **Basic Settings -> Load/Save** (Impostazioni di base -> Carica/Salva) nel campo **Save** (Salva), si seleziona la voce **On the device** (Sul dispositivo) e si fa clic sul pulsante **Save** (Salva).

10.3.5 Priorità QoS, solo per UGM-2040

Se si utilizzano gli switch per la comunicazione tra le reti FPA e l'UGM-2040, la priorità QoS deve essere impostata negli switch dell'UGM.

Nel menu QoS/Priorität -> Global, modificare le impostazioni del campo del menu a discesa in Trusted Mode su trustIpDscp.

Fare clic su **Write** (Scrivi).

**Avviso!**

Le impostazioni delle singole voci di menu nella configurazione degli switch diventeranno effettive dopo aver fatto clic su **Write** (Scrivi).

Le impostazioni vengono salvate solo in maniera permanente, in modo che vengano conservate anche in seguito al riavvio del dispositivo, se in **Basic Settings -> Load/Save** (Impostazioni di base -> Carica/Salva) nel campo **Save** (Salva), si seleziona la voce **On the device** (Sul dispositivo) e si fa clic sul pulsante **Save** (Salva).

10.3.6 Attivazione dello snooping IGMP

Per impedire l'invio di traffico multicast EN 54-2 rilevante ad altri sistemi collegati a Ethernet Switch (Praesideo/PAVIRO, Remote Connect) attivare lo snooping IGMP.

Nella pagina di configurazione IGMP del Ethernet Switch selezionare le opzioni seguenti:

1. Attivare l'utilizzo dello snooping **IGMP**.
2. Attivare **IGMP Querier** (Interrogante IGMP).
3. Configurare l'intervallo di trasmissione, in cui RSR20 invia pacchetti di interrogazioni IGMP (ad es. 4 secondi).
4. Configurare l'intervallo di tempo entro cui i membri del gruppo multicast dovrebbero rispondere alle interrogazioni IGMP (ad es. 3 secondi).
5. Selezionare **Discard** (Annulla) per i pacchetti con indirizzi multicast sconosciuti.
6. Selezionare **Send to Query and registered Ports** (Invia a interrogazione e porte registrate) per i pacchetti con indirizzi multicast conosciuti.

7. Abilitare IGMP solo per le porte in cui sono collegati altri sistemi connessi allo switch.
Disattivare l'opzione **Static Query Port** (Porta interrogazione statica) per tutte le porte.

10.4

Rete CAN

Collegamento in rete ed interfacce

L'unità di controllo della centrale è dotata di

- due interfacce CAN (CAN1/CAN2) per il collegamento in rete (topologia a loop o a linea aperta)
- due ingressi di segnale (IN1/IN2)
- due interfacce Ethernet
- interfaccia USB

A seconda del tipo di unità di controllo della centrale:

- Altre due interfacce Ethernet
- interfaccia RS232

Si noti la lunghezza massima del cavo di 3 m e 2 m rispettivamente per il collegamento all'interfaccia USB e RS232.

Indirizzamento e impostazioni nella rete

A seconda del tipo di unità di controllo della centrale:

- Indirizzo del nodo fisico impostato nel firmware della centrale alla prima accensione della centrale
- RSN su rotary switch meccanici sul lato posteriore della centrale

Per visualizzare l'indirizzo del nodo fisico, se è salvato nell'unità di controllo della centrale:

- ▶ Selezionare **Configurazione -> Servizi di rete -> Ethernet -> Utilizza impostazioni Ethernet -> Impostazioni IP -> Impostazioni pred.**

Per modificare l'indirizzo del nodo fisico salvato nell'unità di controllo della centrale:

- ▶ Visualizzare le impostazioni predefinite e modificare l'ultimo numero dell'**indirizzo IP**.

Per modificare un RSN meccanico:

- ▶ Impostare l'RSN sui rotary switch meccanici posti sul retro della centrale e annotarlo sul segno al di sotto dei rotary switch.

Configurazione della topologia

Gli interruttori DIP per la configurazione di diverse topologie sono situati sul lato posteriore.

- ▶ Contrassegnare l'impostazione selezionata sul segno accanto agli interruttori DIP.

Centrale autonoma e centrale autonoma ridondante

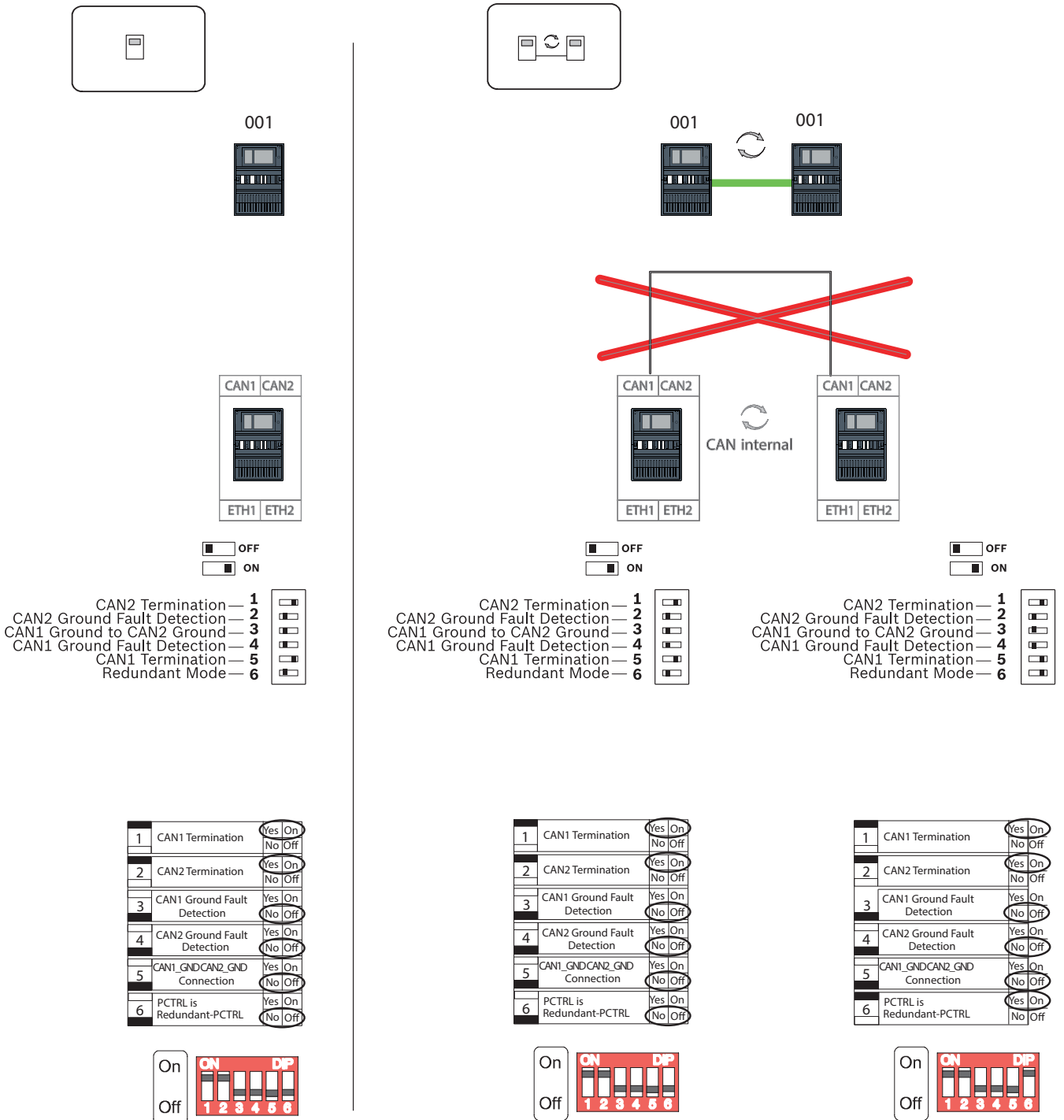
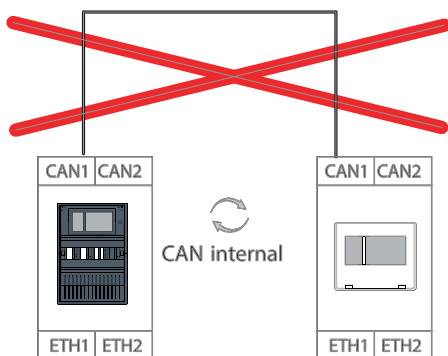
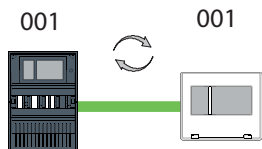
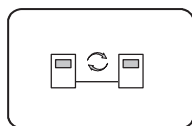


Figura 10.1: Impostazioni DIP switch per centrale autonoma (in alto: AVENAR, in basso: FPA, a sinistra: normale, a destra: ridondante)

Tastierino remoto come centrale ridondante



OFF
 ON

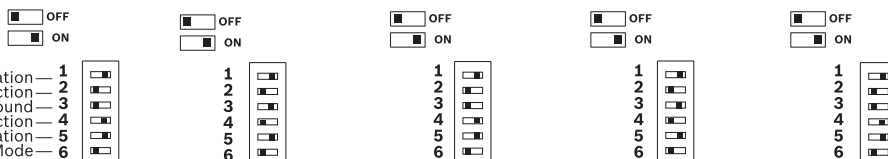
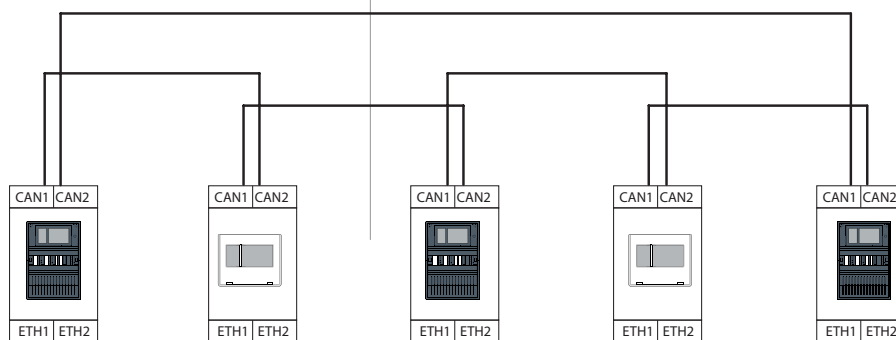
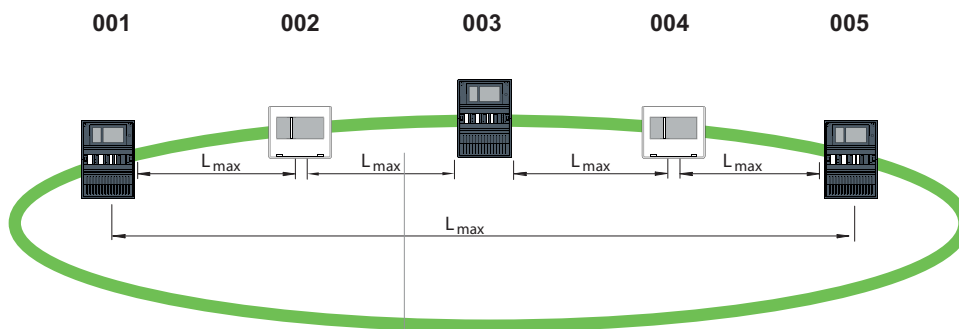
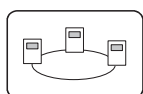
OFF
 ON

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

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

Figura 10.2: Impostazioni DIP switch per tastierino remoto come centrale ridondante (solo AVENAR)

Loop



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

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

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

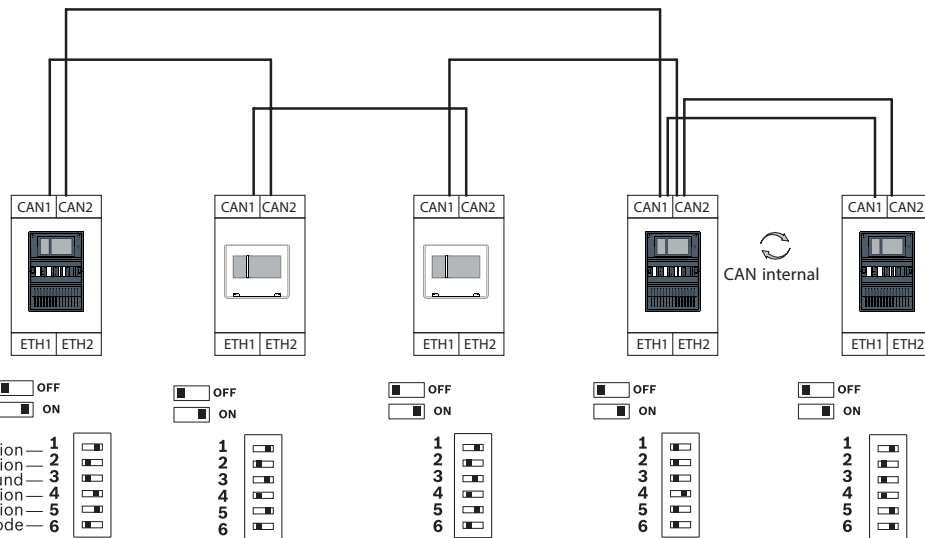
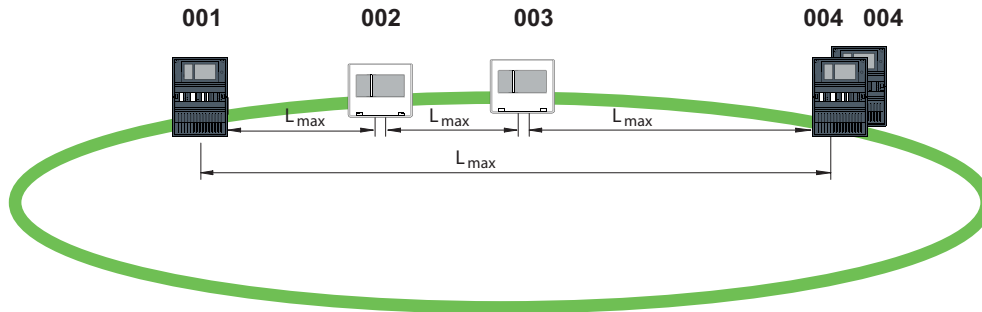
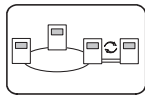
1	CAN1 Termination	Yes/On	No/Off
2	CAN2 Termination	Yes/On	No/Off
3	CAN1 Ground Fault Detection	Yes/On	No/Off
4	CAN2 Ground Fault Detection	Yes/On	No/Off
5	CAN1_GND/CAN2_GND Connection	Yes/On	No/Off
6	PCTRL is Redundant-PCTRL	Yes/On	No/Off

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

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

Figura 10.3: Impostazioni DIP switch per loop (in alto: AVENAR, in basso: FPA)

Loop con centrali ridondanti



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

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

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

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

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

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

On	ON	DIP
Off	1 2 3 4 5 6	

Figura 10.4: Impostazioni DIP switch per loop con centrali ridondanti (in alto: AVENAR, in basso: FPA)

Loop con tastierino remoto come centrale ridondante

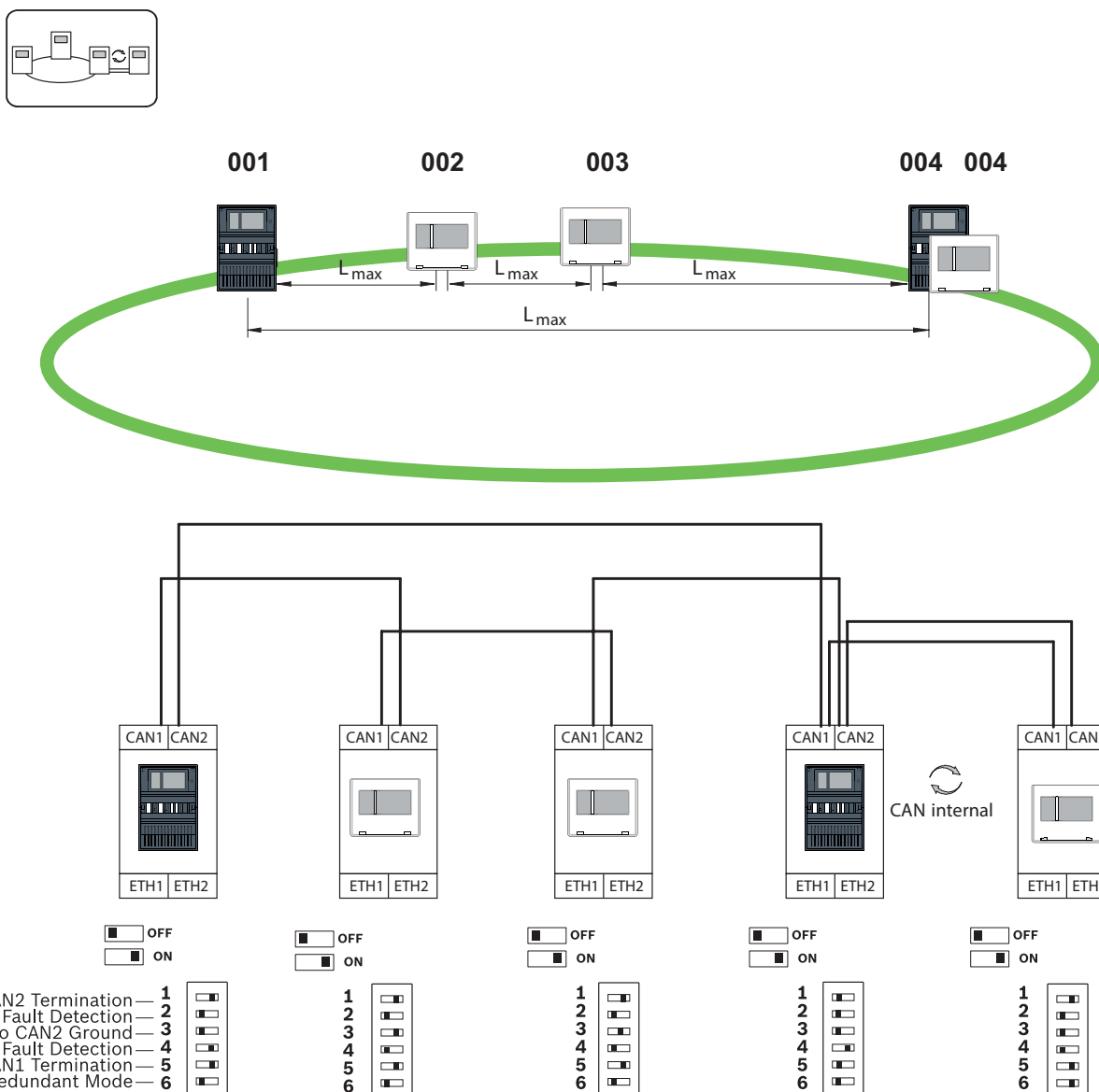


Figura 10.5: Impostazioni DIP switch per loop con tastierino remoto (solo AVENAR)

11 Cablaggio

Per creare un sistema conforme allo standard EN 54-2, gli switch RSTP ed i media converter devono essere collegati tramite alimentazione monitorata della centrale di controllo allarme incendio.

- Per l'alimentazione dei media converter e degli switch RSTP, utilizzare l'uscita a 24 V del modulo BCM 0000 B o FPP-5000.
- Se è stata collegata un'alimentazione ridondante o se si crea un collegamento tra switch, le uscite di guasto degli switch RSTP devono essere monitorate tramite gli ingressi della centrale. Ad esempio, utilizzare gli ingressi sull'unità di controllo della centrale o sul modulo IOP 0008 A.
- Nel caso del media converter, la funzione Link Fault Pass-Through deve essere attivata. La configurazione avviene tramite l'interruttore DIP del media converter.

**Avviso!**

Per il collegamento in rete, utilizzare solo i seguenti cavi:

Cavo Ethernet

Cavo patch Ethernet, schermato, CAT5e o superiore.

Si noti il raggio di curvatura minimo specificato nella sezione relativa al cavo.

Cavo in fibra ottica

Modalità multimodale: cavo patch Ethernet in fibra ottica, duplex I-VH2G 50/125µ o duplex I-VH2G 62,5/125µ, presa SC.

Modalità monodale: cavo patch Ethernet in fibra ottica, duplex I-VH2E 9/125µ, presa SC.

Si noti il raggio di curvatura minimo specificato nella sezione relativa al cavo.

11.1**Convertitore di supporti****Collegamento dei media converter****Avviso!**

Si noti la direzione di trasmissione delle fibre FOC durante il collegamento dei cavi FX dei media converter.

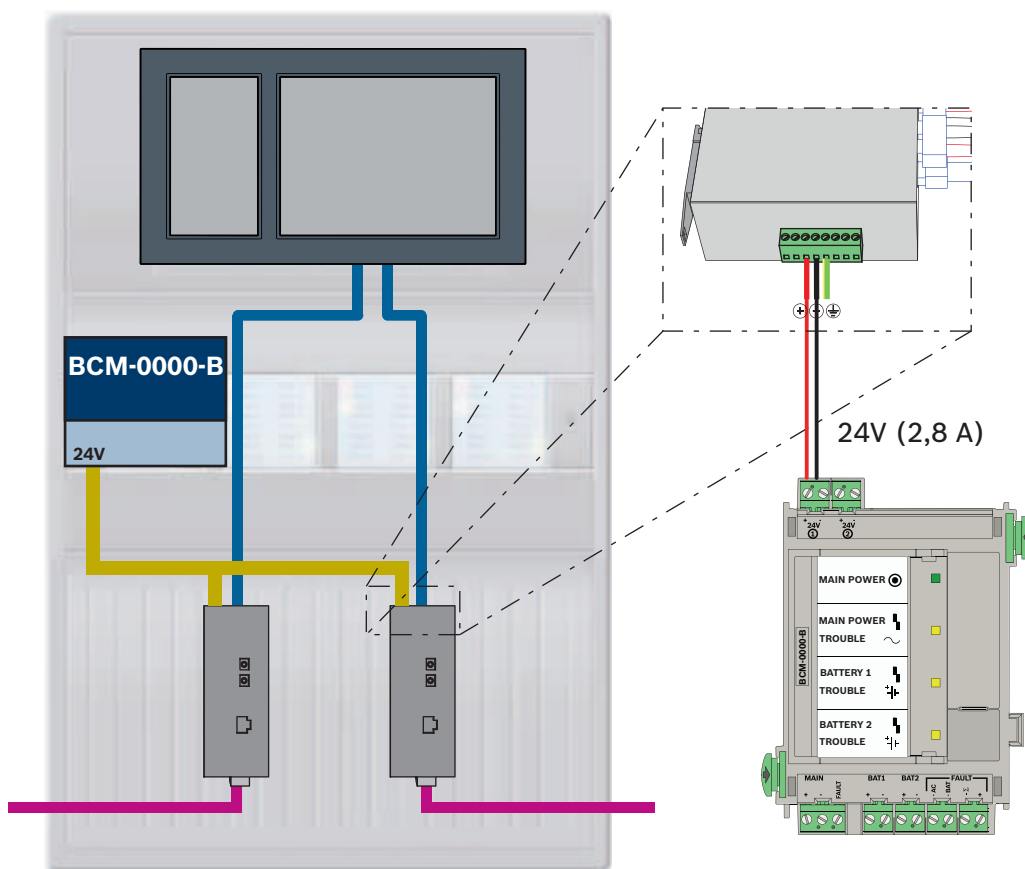





Figura 11.1: Collegamento del media converter all'alimentazione e agli ingressi IN1/IN2 dell'unità di controllo della centrale

Icona	Descrizione
	Cavo Ethernet TX (in rame)
	Cavo Ethernet FX (cavo in fibra ottica)

Icona	Descrizione
	Alimentazione a 24 V
	Trasmissione del guasto
	Media converter

11.2 Switch Ethernet

Collegamento dello switch

È possibile collegare le uscite di guasto degli switch agli ingressi dell'unità di controllo della centrale o a un modulo di uscita o ingresso IOP.



Avviso!

Il relè di guasto deve essere collegato per applicazioni che soddisfano almeno uno dei seguenti requisiti:

Esiste un collegamento tra due switch. Ciò è possibile in caso di anello principale con loop secondari, ed esempio.

L'alimentazione dello switch è progettata come ridondante.

Collegamento degli switch con report dei guasti agli ingressi del modulo IOP:

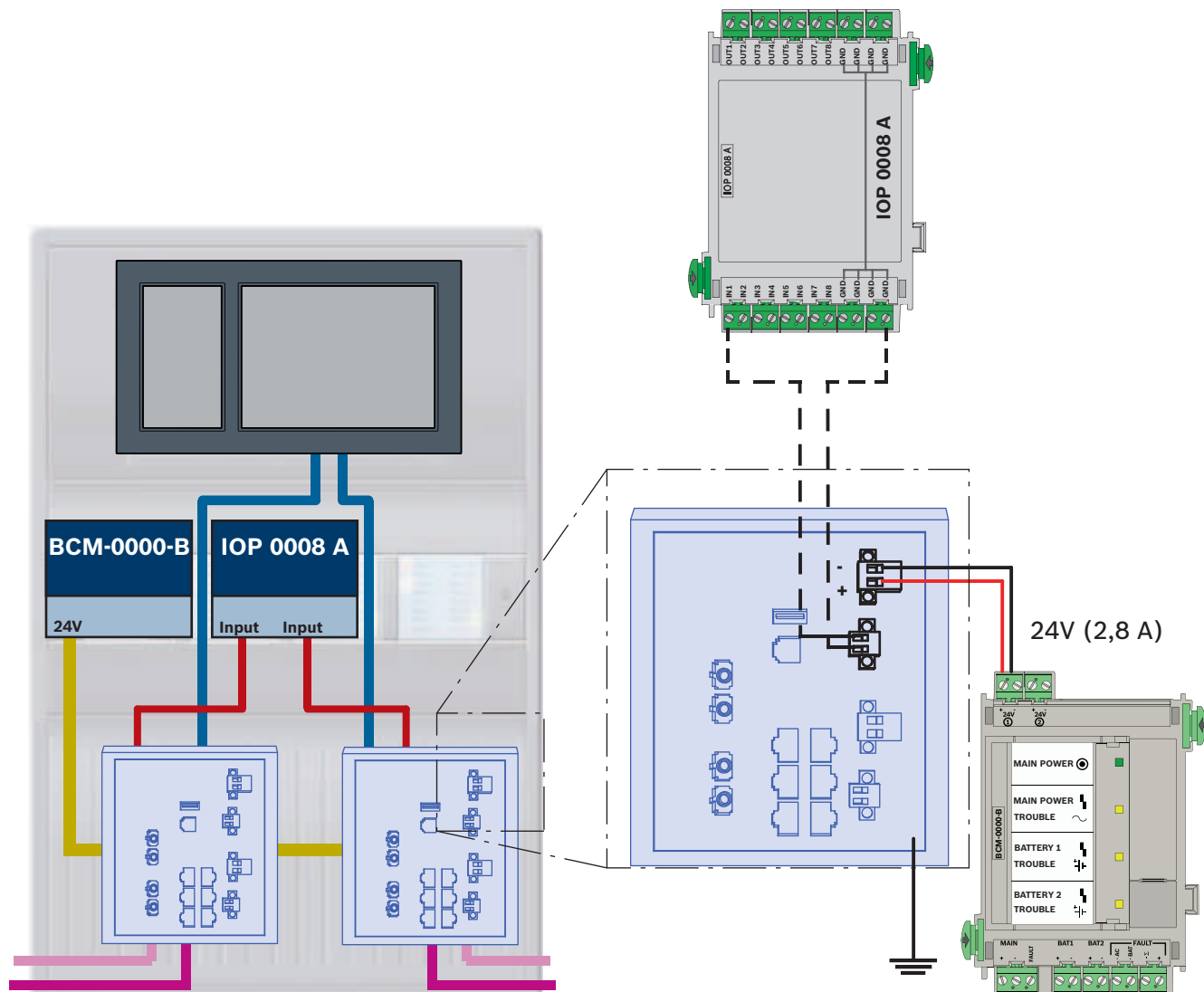


Figura 11.2: Collegamento dello switch all'alimentazione ed a IOP.

Icona	Descrizione
	Cavo Ethernet TX (in rame)
	Cavo Ethernet FX (cavo in fibra ottica)
	Alimentazione a 24 V
	Trasmissione del guasto
	Switch RSTP

Collegamento degli switch con report dei guasti agli ingressi dell'unità di controllo della centrale

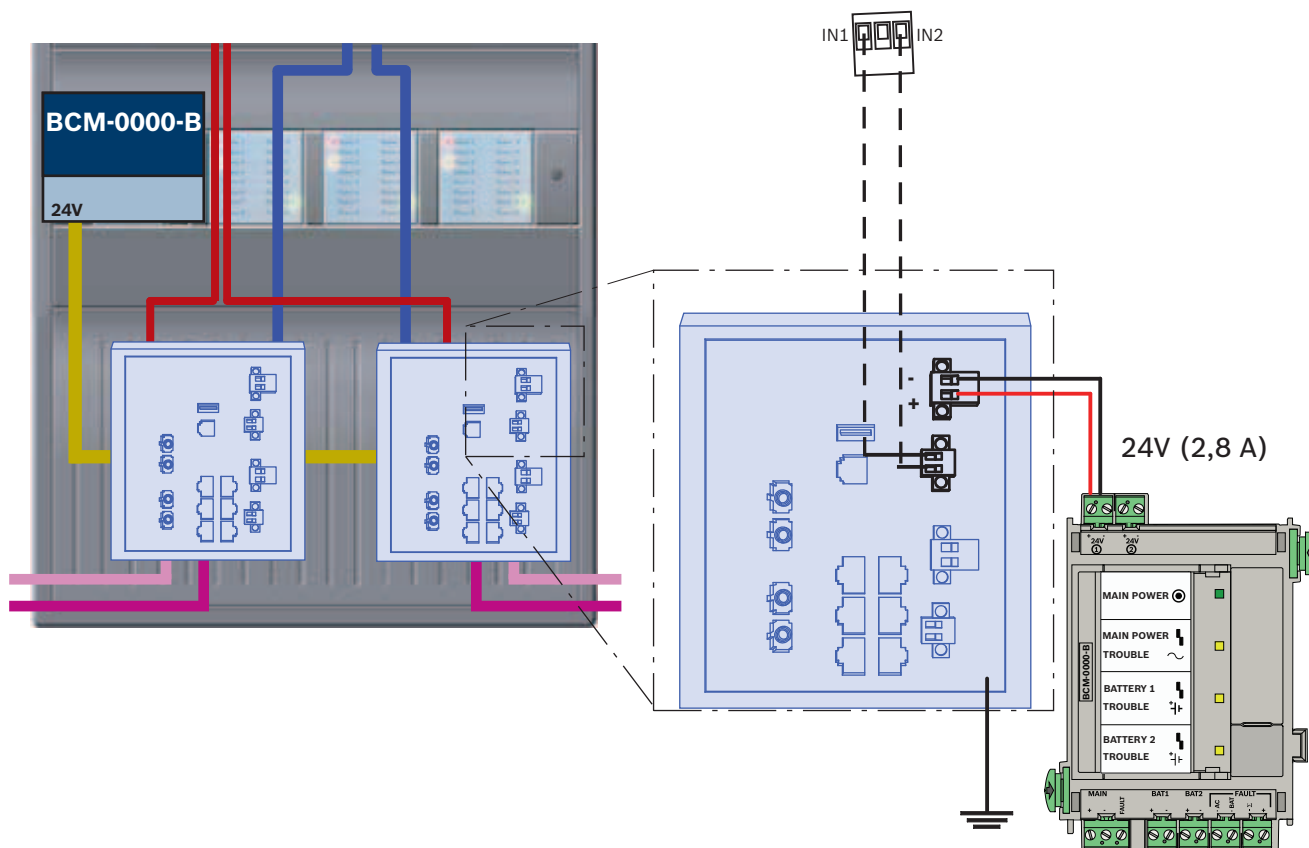


Figura 11.3: Collegamento dello switch all'alimentazione ed all'unità di controllo della centrale

Icona	Descrizione
	Cavo Ethernet TX (in rame)
	Cavo Ethernet FX (cavo in fibra ottica)
	Alimentazione a 24 V
	Trasmissione del guasto
	Switch RSTP



Avviso!

Non utilizzare il cavo di rete fornito in dotazione per collegare gli switch. Utilizzare un cavo patch Ethernet, schermato, CAT5e o superiore.

11.3 Tastierino remoto

Un tastierino remoto deve essere alimentato tramite alimentatore FPP-5000 esterno. Il collegamento alla rete viene stabilito attraverso 2 media converter in PSS 0002 A o USF 0000 A

**Avviso!**

Si noti che l'alimentatore FPP-5000 esterno e PSF 0002 A (PSS 0002 A) devono essere installati nelle immediate vicinanze (senza barriere intermedie) del tastierino remoto. Non deve essere possibile toccare i cavi di collegamento tra i componenti, perché non è previsto il monitoraggio dei cortocircuiti e delle interruzioni di circuito lente.

**Avviso!**

Utilizzare solo i media converter per il collegamento di un tastierino remoto a una rete di centrali Ethernet.

L'utilizzo degli switch non è consentito per il tastierino remoto.

**Avviso!**

La messa a terra funzionale del tastierino remoto deve essere sempre indicata durante il collegamento dell'unità a una rete di centrali Ethernet.

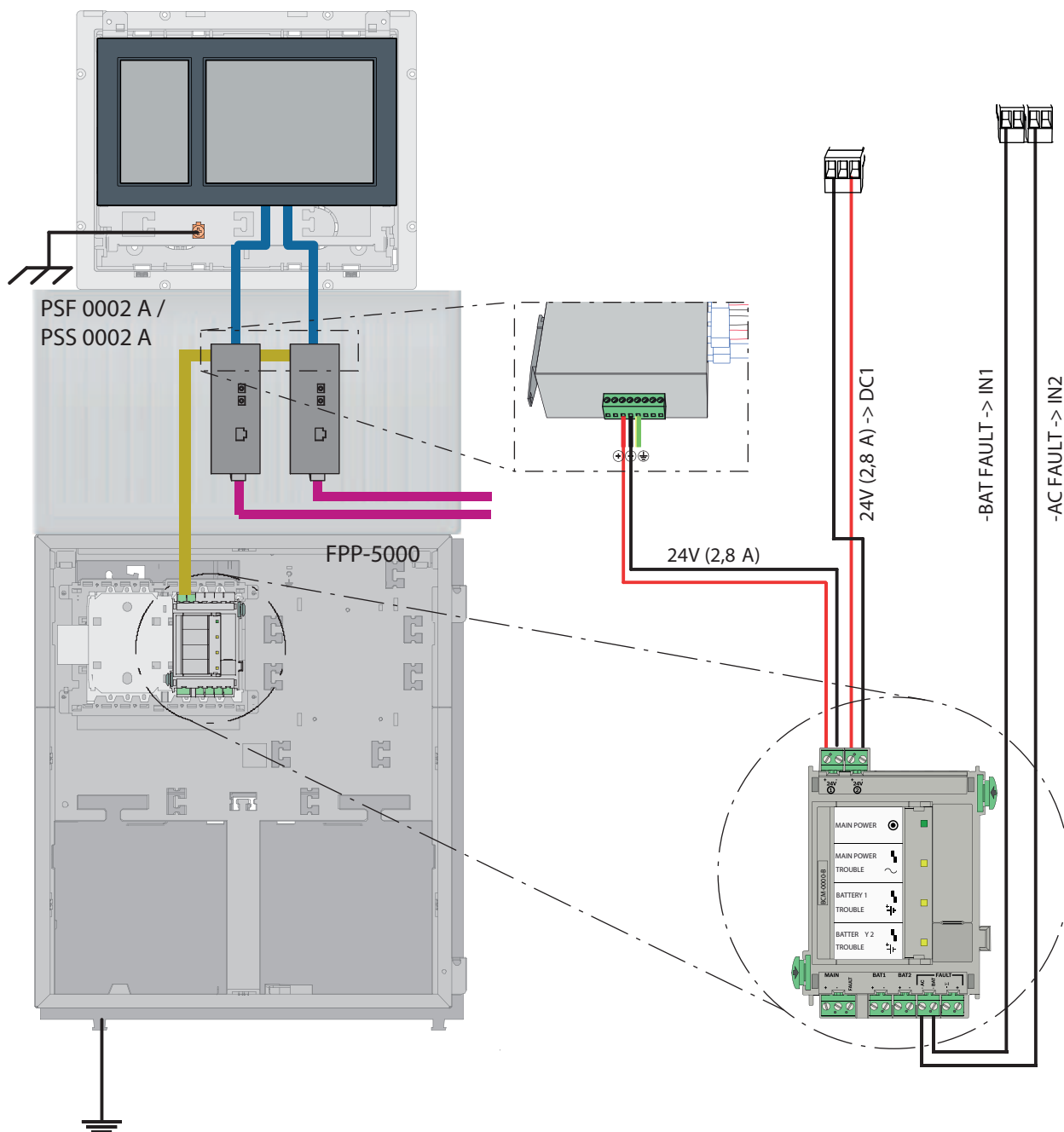






Figura 11.4: Cablaggio del tastierino remoto

Icona	Descrizione
	Cavo Ethernet TX (in rame)
	Cavo Ethernet FX (cavo in fibra ottica)
	Alimentazione a 24 V
	Media converter

12 Impostazioni FSP-5000-RPS

È possibile programmare l'intera rete con il software di programmazione RPS tramite la porta USB, l'interfaccia di rete o l'interfaccia seriale di una centrale. Per fare questo, è necessario che le impostazioni di rete vengano configurate sulla centrale e riavviate affinché la rete venga messa in funzione.

In alternativa, è possibile utilizzare l'interfaccia di rete di uno switch collegato alla rete.

12.1 Nodi di rete

È necessario programmare l'intera rete con tutti i nodi di rete nel software di programmazione FSP-5000-RPS e caricare il tutto sulla rete. Per effettuare questa operazione, procedere come indicato di seguito:

- Collegare i nodi FPA
 - Impostare la RSN nei singoli nodi
- Regolare i numeri delle linee del cablaggio di rete in modo da creare la topologia prevista
- Controllare la topologia visualizzata per accertarsi che sia corretta
- Se necessario, collegare il server OPC, il sistema Praesideo/PAVIRO, il server UGM-2040 e gli switch
- Modificare la configurazione IP ed Ethernet
 - Assegnare gli indirizzi IP o utilizzare le impostazioni standard se si utilizza una topologia con un numero di switch RSTP inferiore a 20
 - Scegliere il protocollo di ridondanza appropriato per la topologia impostata
- Eseguire un controllo della consistenza
- Collegarsi alla rete tramite Ethernet, USB o interfaccia seriale
- Completare un accesso multiplo
- Effettuare un autorilevamento completo per ciascuna centrale
- Richiedere le informazioni di configurazione e completare tutte le operazioni

Controllare i messaggi di errore dopo il riavvio della rete e rettificare eventuali errori, se necessario.

12.2 Numeri delle linee

È necessario assegnare un numero di linea a ciascun collegamento in rete in uso. Non è rilevante se si tratta di una connessione CAN o Ethernet.

È possibile utilizzare un numero di linea sia per una connessione CAN che per una connessione Ethernet. Tuttavia, per facilitare la visualizzazione dei collegamenti, è necessario utilizzare diversi intervalli di numeri.

Se si utilizza come nella finestra , il numero di linea deve essere 0 per tutte le connessioni.

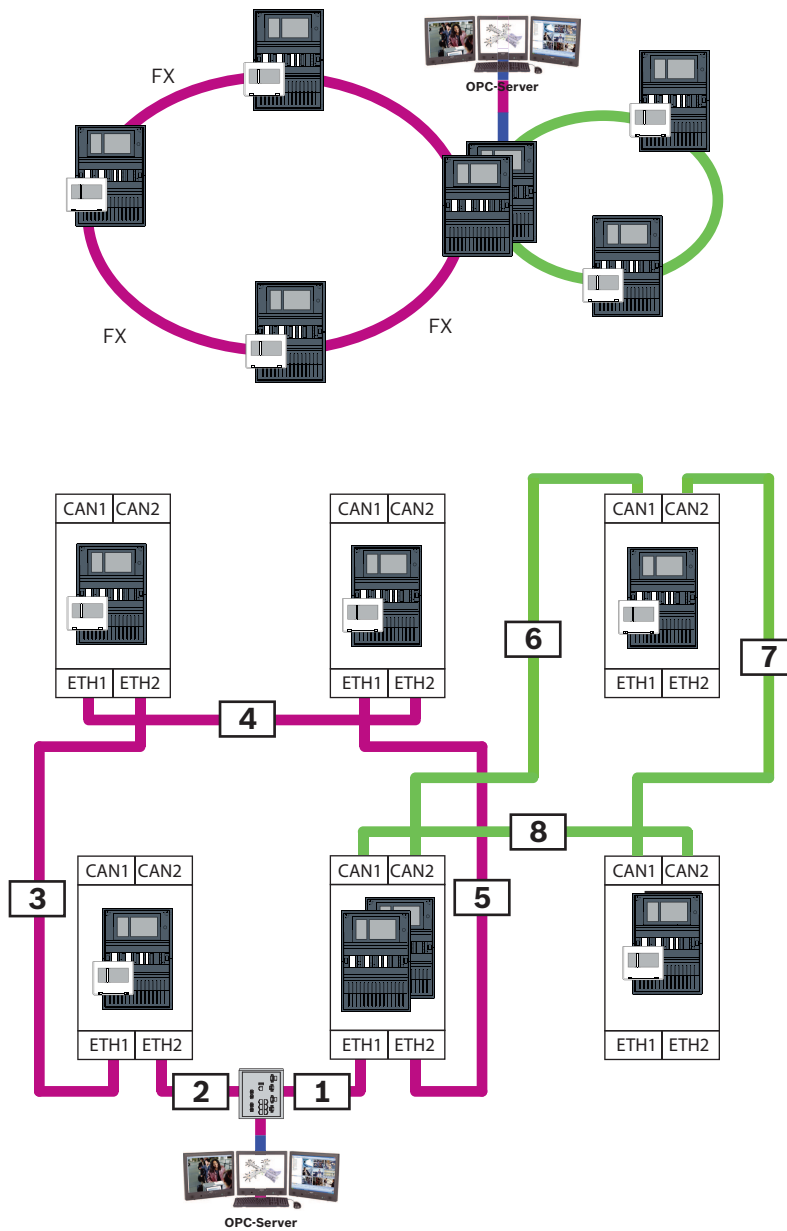


Figura 12.1: Esempio di una rete e della possibile numerazione delle linee

12.3 Switch

Se nella rete si utilizzano switch, questi devono essere creati nel software di programmazione FSP-5000-RPS. È possibile assegnare un massimo di 128 porte a ciascuno switch creato. Per creare la rete, è possibile assegnare i numeri delle linee collegate alle singole porte.

12.4 Server OPC

I server OPC nella rete devono essere aggiunti al software di programmazione FSP-5000-RPS. È necessario effettuare le seguenti impostazioni sia nel software FSP-5000-RPS che sul server OPC:

- Nodi di rete
- Gruppo di rete
- RSN
- Indirizzo IP
- Porta

Il server OPC utilizza la porta 25000 come standard.

**Avviso!**

EN 54

Il collegamento di un sistema di gestione edifici (ad esempio BIS) tramite un'interfaccia Ethernet utilizzando un server OPC o un server FSI è conforme a EN 54 se le funzioni relative a EN 54 vengono eseguite esclusivamente dalla centrale antincendio. Qualsiasi attività di controllo o amministrazione relativa a EN 54 (ad esempio il controllo degli apparecchi di notifica o l'amministrazione dello spegnimento) da parte del sistema di gestione edifici richiede una certificazione EN 54 individuale dell'intero sistema da parte di un ente di certificazione.

**Avviso!**

Software di programmazione FSP-5000-RPS

È necessario assegnare un server OPC a ciascun nodo di rete da cui vengono trasmessi gli stati.

12.5**Server UGM-2040**

**Avviso!**

Tutte le unità di controllo della centrale ed i server UGM devono trovarsi nella stessa sottorete e devono avere lo stesso indirizzo multicast.

Nel caso di più reti o configurazioni di centrali, queste devono trovarsi nella stessa sottorete. Gli indirizzi multicast deve essere differenti.

**Avviso!**

È necessario assegnare il server UGM-2040 a ciascun nodo di rete da cui vengono trasmessi gli stati.

Per collegare una centrale all'UGM-2040, è necessario simulare la struttura fisica della rete in RPS. Ciò include anche i numeri delle linee tra l'unità di controllo della centrale collegata e gli interruttori dell'UGM-2040.

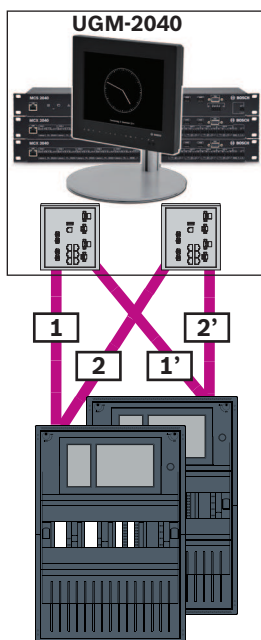


Figura 12.2: Esempio di numerazione delle linee per l'UGM-2040

13 Appendice

13.1 Messaggi di errore Ethernet

Si noti che, in caso di errore, il messaggio di errore e l'errore del gruppo vengono visualizzati in ciascuna istanza.

Indirizzo fisico	Indirizzo logico	Messaggio di errore	Descrizione e possibile causa
Guasti del gruppo correlati al malfunzionamento generale della rete			
135.0.1.0	Rete 1.0		Esiste una versione non compatibile del software della rete di centrali. Le versioni del software disponibili sono due
Guasti del gruppo correlati alla rete			
135.0.6.1	Rete 2.1		Un indirizzo IP è stato assegnato due volte.
135.0.6.2	Rete 2.2		La configurazione IP della centrale di segnalazione è differente dalla configurazione RPS
135.0.6.3	Rete 2.3		La configurazione di ridondanza (RSTP, parametro RSTP, dual-homing o nulla) della centrale di segnalazione è differente dalla configurazione RPS.
Guasti del gruppo correlati a Rapid Spanning Tree Protocol (RSTP)			
135.0.7.1	Rete 3.1		La centrale di segnalazione è passata dalla modalità RSTP alla modalità STP (modalità di compatibilità). Un dispositivo STP è stato collegato alla rete.
135.0.7.2	Rete 3.2		La topologia di rete RSTP è stata modificata. Ad esempio, è stato aggiunto un altro dispositivo RSTP alla rete. Questo messaggio potrebbe essere visualizzato anche in caso di interruzione della linea.

Indirizzo fisico	Indirizzo logico	Messaggio di errore	Descrizione e possibile causa
135.0.7.3	Rete 3.3		Una porta RSTP della centrale di segnalazione non si trova nello stato point-to-point. Ad esempio, sono stati collegati diversi dispositivi RSTP a una porta RSTP. Oppure un altro dispositivo RSTP è stato collegato alla porta RSTP tramite linea half-duplex.
Guasti del gruppo correlati alla connessione di rete			
135.0.5.1	Connessione di rete 1.0		La trasmissione dati al bus CAN 1 è limitata. Cause possibili: danneggiamenti, mancati collegamenti o interferenza dei cavi.
135.0.5.2	Connessione di rete 2.0		La trasmissione dati al bus CAN 2 è limitata. Cause possibili: danneggiamenti, mancati collegamenti o interferenza dei cavi.
135.0.5.3	Connessione di rete 3.0		La trasmissione dati alla linea Ethernet 1 è limitata. Cause possibili: danneggiamenti, mancati collegamenti o interferenza dei cavi.
135.0.5.4	Connessione di rete 4.0		La trasmissione dati alla linea Ethernet 2 è limitata. Cause possibili: danneggiamenti, mancati collegamenti o interferenza dei cavi.

Indice

C

Collegamento in rete	
Lunghezza cavo	26
Topologia loop	26
Collegamento in rete su CAN	8
Collegamento in rete su TCP/IP	8

D

Diametro della rete	22
---------------------	----

E

Ethernet, impostazioni standard	13
---------------------------------	----

G

Gateway di rete sicuro	35, 39
------------------------	--------

I

Impostazioni standard, Ethernet	13
Indirizzamento	
Indirizzo del nodo fisico	12
Indirizzo del nodo fisico	12
Indirizzo MAC	21
Interfaccia CAN	12, 48
Interfaccia Ethernet	48
Interfaccia RS232	48
Interfaccia USB	48

L

Limite massimo	12
Limiti: Rete	12
LLDP	21

P

Parametri	
RSTP	13, 14
Parametri RSTP	13, 14
PAVIRO	8, 41, 42
Praesideo	8, 41, 42

R

Remote Alert	37
Remote Connect	35
Remote Maintenance	37
per Remote Portal	37
per rete privata protetta	38
Remote Portal	37, 39

Remote Services	35, 39
Assegnazione di una licenza	41
Connessione del gateway di rete sicuro	39
Creazione di un account Remote Portal	39
Creazione di una connessione remota	41
Licenza	41
Nuovo ordine della licenza	41
Separazione delle sottoreti	40

Rete

Cavo	26, 27
Indirizzamento	51
Limiti	12
Rete CAN	8
Rete Ethernet	8
Rete: Cablaggio	26, 27
Rete: Unità di controllo della centrale	48
Ridondanza	
Indirizzamento	12
RSN	12
RSTP	22

S

Server OPC	8, 48
Servizi	8
Sistema di allarme vocale	41, 42

T

Topologie CAN	10
Topologie Ethernet	10
Topologie, CAN	10
Topologie, Ethernet	10

U

Unità di controllo della centrale	
Collegamento in rete	48



Bosch Sicherheitssysteme GmbH

Robert-Bosch-Ring 5

85630 Grasbrunn

Germany

www.boschsecurity.com

© Bosch Sicherheitssysteme GmbH, 2020