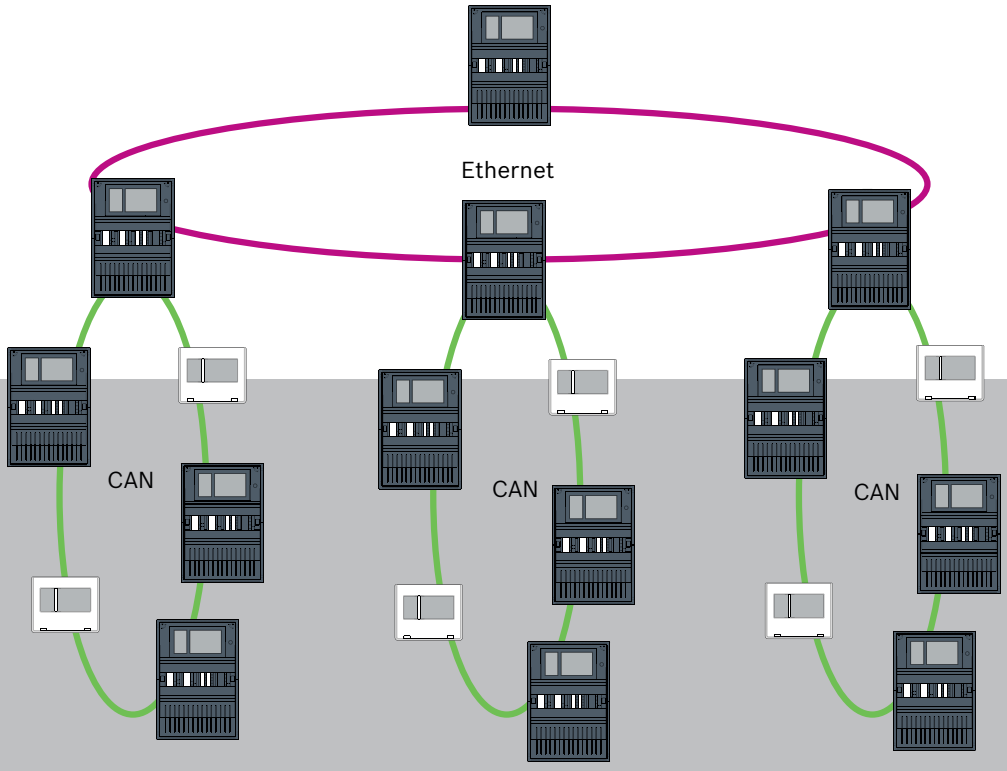
AVENAR panel | FPA-5000 | FPA-1200



nl Networking manual

Inhoudsopgave

1 Veiligheid

In dit hoofdstuk vindt u organisatorische maatregelen voor pc's waarop service-clients worden uitgevoerd voor de Bosch portfolio met branddetectieproducten. U bent verplicht deze contractuele overeenkomsten na te leven.
U treft in deze handleiding tevens veiligheidsaanwijzingen aan die op onderwerp zijn verzameld en gesorteerd. Verderop worden deze veiligheidsaanwijzing voor de relevante instructie geplaatst.

1.1 Organisatorische maatregelen voor pc's waarop service-clients worden uitgevoerd

Inleiding

De Bosch portfolio voor branddetectieproducten omvat pc-programma's (service-clients) die worden uitgevoerd op een computer, en die een fysieke verbinding met het branddetectiesysteem vereisen. Vanuit het oogpunt van veiligheid en regelgeving mag het branddetectiesysteem niet worden geïnstalleerd in een gedeeld netwerk. Dit betekent dat het volledige netwerk van het branddetectiesysteem en de pc waarop een service-client wordt uitgevoerd een fysiek toegewezen netwerk moeten vormen. Aangezien Bosch alleen de service-clients ontwikkelt en niet de pc's waarop deze worden uitgevoerd, heeft Bosch geen controle over de computer. Om het risico van mogelijke beveiligingsproblemen te beperken, worden in deze documenten organisatorische maatregelen beschreven.

Maatregelen

Als voor de hierna beschreven maatregelen een internetverbinding vereist is - of de service-client een tijdelijke internetverbinding vereist voor licentiedoelen, moet de pc fysiek zijn losgekoppeld van het netwerk van het branddetectiesysteem voordat de pc met internet wordt verbonden. De internetverbinding moet worden verwijderd voordat de pc weer met het netwerk van het branddetectiesysteem wordt verbonden.

1. Besturingssystemen
   Bosch documenteert de vereisten voor de service-clients, waaronder de versie van het besturingssysteem. De clients zijn gegarandeerd compatibel met deze versies. Het besturingssysteem waarop de client wordt uitgevoerd, moet regelmatig worden bijgewerkt om mogelijke zwakke plekken in de beveiliging te corrigeren.
   Het systeem moet zodanig worden geconfigureerd dat alleen toegang mogelijk is tot de mappen die vereist zijn voor de desbetreffende taak. Standaard worden aan alle gebruikers alleen-lezenrechten verleend.
2. Antivirus
   Geavanceerde antivirussoftware moet op de computer zijn geïnstalleerd en worden uitgevoerd. De definitiebestanden van de antivirussoftware moeten regelmatig worden bijgewerkt.
3. Firewall
   Op de pc moet een software-firewall zijn geïnstalleerd en worden uitgevoerd. Deze moet zodanig zijn geconfigureerd dat verkeer tussen de service-client en het branddetectiesysteem, updates voor het besturingssysteem en de antivirussoftware worden toegestaan. Daarnaast moet de firewall al het overige verkeer blokkeren.
4. Beveiligde gebruikersaanmelding
   De toegang tot de pc moet beperkt zijn tot de operators die de geïnstalleerde service-client gebruiken. De aanmelding moet worden beveiligd met gebruikmaking van geavanceerde middelen. Als de toegang wordt beveiligd met een wachtwoord, moeten

geavanceerde wachtwoordregels worden afgedwongen door wachtwoordbeleid. Indien van toepassing, is verificatie met de tweemansregel (vier-ogenprincipe) of meerdere factoren een aanbevolen benadering om de verificatie te versterken.

5. Software en services
   Er moet zo min mogelijk software worden geïnstalleerd op de pc. Alleen software die vereist is voor de service-client en voor bijbehorende taken dient te worden geïnstalleerd.
6. Gebruiksbeperkingen
   Het gebruik van de pc moet via organisatorische middelen worden beperkt tot servicegerelateerde taken. Deze beperking geldt tevens voor internetgebruik voor andere doelen dan degene die in dit document zijn beschreven.
7. Scheiding van taken
   Taken en verantwoordelijkheidsgebieden dienen gescheiden te worden om mogelijkheden voor ongeautoriseerde of onbedoelde wijzigingen of misbruik te beperken. Dit betekent dat verschillende taken moeten worden toegewezen aan verschillende rollen.
8. Bewaking
   Alle pogingen tot toegang tot de pc waarop de service-client wordt uitgevoerd, moeten worden bewaakt om vast te kunnen stellen wanneer er sprake is van ongeautoriseerde toegang tot de pc en internet.

1.2 Toelichtingen van veiligheidssymbolen

Waarschuwing!
Wijst op een gevaarlijke situatie die, indien deze situatie niet wordt vermeden, kan leiden tot de dood of ernstig letsel.

Voorzichtig!
Wijst op een gevaarlijke situatie die, indien deze situatie niet wordt vermeden, kan leiden tot licht of middelzwaar letsel.

Opmerking!
Wijst op een situatie die, indien deze situatie niet wordt vermeden, kan leiden tot schade aan de apparatuur of de omgeving, of verlies van gegevens.

1.3 Veiligheidsaanwijzingen

Mediaconverter

Waarschuwing!
Laserlicht
Kijk niet rechtstreeks in de straal met het blote oog of met visuele instrumenten (zoals een vergrootglas of microscoop). Als u dat toch doet, is dat gevaarlijk voor uw ogen op een afstand van minder dan 100 mm. Het licht komt tevoorschijn bij de visuele klemmen of aan het einde van de glasvezelkabels die hierop zijn aangesloten. Lichtgevende diode van klasse 2M, golflengte 650 nm, uitgang < 2 mW, voldoet aan IEC 60825-1.

Remote Services

Voorzichtig!
Gebruik voor toegang via internet uitsluitend BoschRemote Services.

Voorzichtig!
Voor Remote Services is een beveiligde IP-verbinding vereist. Bosch Remote Services of een verbinding met Private Secure Network is vereist.
Bij gebruik van Private Secure Network hebt u de beschikking over een IP-netwerk dat is gebaseerd op DSL met optioneel draadloze toegang aan de kant van de centrale (EffiLink). Remote Services voor Private Secure Network is alleen beschikbaar in Duitsland met een serviceovereenkomst met Bosch BT-IE.

Opmerking!
Er is een exclusief (enkel voor FPA-5000) Ethernet-netwerk vereist voor het instellen van een netwerk met FPA-5000 brandmeldcentrales.
Het gebruik van een brandalarmsysteem in elk ander Ethernet-netwerk is voor risico van de gebruiker. Bosch wijst alle garanties en aansprakelijkheid af voor onjuiste toepassingen.
Bij gebruik van een niet-exclusief Ethernet-netwerk kunnen geen betrouwbare alarmtransmissie en IT-beveiliging worden gegarandeerd.

Smart Safety Link

Waarschuwing!
Ethernet-beveiligingsrisico's
Sluit PRAESENSA niet aan op FPA-5000/FPA-1200 met Smart Safety Link vanwege Ethernet-beveiligingsrisico's.

Opmerking!
VdS 2540
Het gesproken woord ontruimingssysteem moet samen (tegen elkaar) met de brandmeldcentrale (BMC) worden opgesteld in één en dezelfde ruimte. Anders wordt niet voldaan aan de vereisten van VdS 2540 voor gegevenstransmissiekanalen.

Centralenetwerk

Opmerking!
EN 54
Gebruik alleen onderdelen die zijn goedgekeurd voor gebruik in centrale brandalarmnetwerken, om er zeker van te zijn dat het netwerk voldoet aan EN 54.
Externe RSTP-switches en media-omvormers in Ethernet-netwerken moeten worden geïnstalleerd in behuizingen van centrales. Installaties buiten de centralebehuizing voldoen niet aan EN 54.

Opmerking!
TX-kabellengte
Alle IP-verbindingen moeten direct zijn of via media-omvormers die zijn goedgekeurd door Bosch. De TX-kabellengte van knooppunt tot knooppunt moet minder zijn dan 100 m.

Opmerking!
VdS 2540
Gebruik glasvezelkabel voor Ethernet-verbindingen om te voldoen aan de vereisten van VdS 2540 voor gegevenstransmissiekanalen. Voor verbindingen binnen een behuizing kunnen TX Ethernet-kabels worden gebruikt.

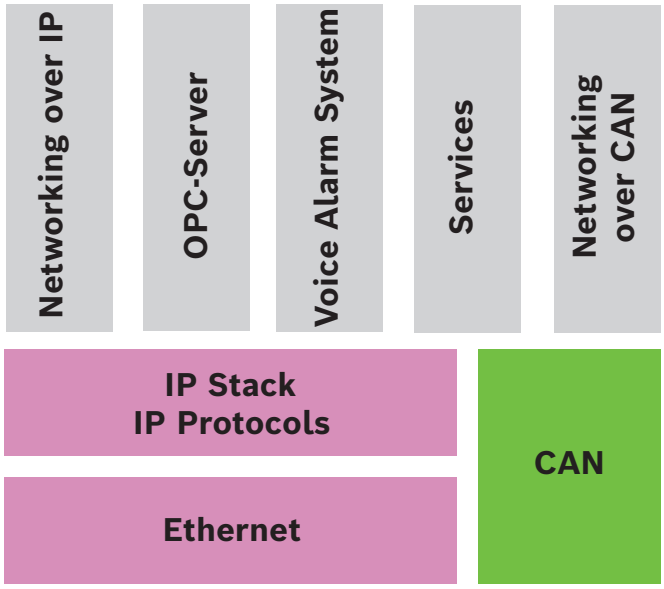
Opmerking!
Gebruik voor standaardtoepassingen standaardnetwerkinstellingen.
Wijzigingen in de standaardnetwerkinstellingen mogen alleen worden aangebracht door ervaren gebruikers met een goede kennis van netwerken.

Opmerking!
Toepasselijke topologieën
De functionaliteit en de communicatie tussen centrales worden beperkt door het centraletype. Raadpleeg de specificaties van de centrale voor informatie over services, het aantal centrales dat kan worden aangesloten en het aantal externe bedieningspanelen dat kan worden aangesloten.

2 Inleiding

Dit document is bestemd voor lezers die ervaring hebben met het plannen en installeren van brandalarmsystemen die voldoen aan EN 54. Ook kennis van netwerken is noodzakelijk.
In dit document worden uiteenlopende netwerktopologieën voor brandalarmen beschreven. De topologieën worden onafhankelijk van het type brandmeldcentrale beschreven.
Voor het opbouwen van centralenetwerken overeenkomstig de geïntroduceerde topologieën en verbindingsservices, is het netwerkpatroon vereist dat in dit document wordt beschreven.
Het document bevat een overzicht van de basisvoorwaarden, limietwaarden en algemene procedures voor de planning en installatie van het netwerk voor een centrale.
Gedetailleerde omschrijvingen van de installatie van de afzonderlijke onderdelen kunt u vinden in de installatiehandleidingen van die onderdelen.
U vindt een omschrijving van de gebruikersinterface van de paneelcontroller in de gebruikershandleiding die bij het apparaat hoort.
De gebruikersinterface van de programmeersoftware FSP-5000-RPS wordt beschreven in de online-Help.

3 Systeemoverzicht



In het netwerk worden de Ethernet-interface en de IP-protocollen gebruikt voor verschillende services. De Ethernet-interface kan volledig worden uitgeschakeld of alleen worden uitgeschakeld voor netwerken via TCP/IP. Uitschakelen kan noodzakelijk zijn voor netwerken via CAN.

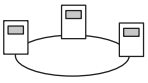
Services inschakelen

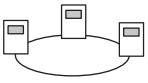
- netwerken via TCP/IP
  In FSP-5000-RPS de communicatie tussen centrales in het Ethernet-netwerk inschakelen
- OPC-servers
  Een OPC-server toevoegen aan de FSP-5000-RPS-configuratie
- Aansluiting op gesproken woord ontruimingssysteem
  Een ontruimingssysteem toevoegen aan de FSP-5000-RPS-configuratie en virtuele activeringen configureren.
- Remote Services (Remote Connect als vereiste, Remote Maintenance en Remote Alert)
  Het relevante selectievakje inschakelen in FSP-5000-RPS
- Remote Services (Remote Connect als vereiste, Remote Maintenance en Remote Alert) voor Private Secure Network
  Externe toegang toevoegen aan de FSP-5000-RPS-configuratie en de externe toegang instellen in FSP-5000-RPS.

Opmerking!
Onbedoelde gegevensoverdracht
Als de Ethernet-interface van de paneelcontroller alleen wordt gebruikt voor communicatie met een OPC-server of voor Remote Services, schakelt u de communicatie tussen centrales via TCP/IP uit in FSP-5000-RPS. Anders kunnen er onbedoeld gegevens over brandmeldingen worden verzonden via Ethernet.

Voor het gebruik van Ethernet- of TCP/IP-services moeten de Ethernet-interfaces zijn ingeschakeld en de juiste TCP/IP-instellingen zijn geconfigureerd.

Netwerk van centrales en externe bedieningspanelen
In de tabel worden de opties weergegeven voor het verbinden van centrales/externe bedieningspanelen in een netwerk, afhankelijk van de netwerktopologie en het type centrale. Houd rekening met de limieten die worden bepaald door de netwerktopologie.

Topologie	**AVENAR panel 8000, premiumlicentie**	**AVENAR panel 8000, standaardlicentie**	**AVENAR panel 2000, premiumlicentie**	**AVENAR panel 2000, standaardlicentie**
 Zelfstandig	Mogelijk	Mogelijk	Mogelijk	Mogelijk
 Lus	Max. 32 centrales/externe bedieningspanelen, connectiviteit met AVENAR panel 2000, premiumlicentie en FPA	Max. 32 centrales/externe bedieningspanelen, connectiviteit met AVENAR panel 2000, premiumlicentie en FPA	Max. 32 centrales/externe bedieningspanelen, connectiviteit met AVENAR panel 8000 en FPA	1 centrale en max. 3 externe bedieningspanelen
 Centrale-redundantie	Redundante paneelcontroller moet tevens premium zijn. Ook een extern bedieningspaneel kan als redundante centrale worden gebruikt.	Redundante paneelcontroller kan standaard zijn. Ook een extern bedieningspaneel kan als redundante centrale worden gebruikt.	Niet mogelijk	Niet mogelijk

Topologie	**FPA-5000**	**FPA-1200**
 Zelfstandig	Mogelijk	Mogelijk
 Lus	Max. 32 centrales en externe bedieningspanelen	1 centrale en max. 3 externe bedieningspanelen
 Centrale-redundantie	Mogelijk	Niet mogelijk (DIP 6 op paneelcontroller is niet functioneel.)

Als u een FPA-5000-netwerk uitbreidt, raadt Bosch aan het netwerk uit te breiden met een centrale van de AVENAR panel-serie.

Wanneer u een centrale van de FPA-serie vervangt door een centrale van de AVENAR panel-serie, hoeft alleen de paneelcontroller te worden vervangen. Denk eraan dat de centrales van de AVENAR panel-serie geen adreskaarten ondersteunen. Als een Ethernet-switch is aangesloten, kunt u deze blijven gebruiken.

Controleer, wanneer u een extern bedieningspaneel van de FPA-serie vervangt door een extern bedieningspaneel van de AVENAR panel-serie, of de lijnweerstand binnen het bereik ligt dat is gespecificeerd voor het externe bedieningspaneel van de AVENAR panel-serie.

Opmerking!
Installatie van de firmware
Verbonden centrales moeten dezelfde firmwareversie hebben.
Installatie van de firmware is alleen mogelijk voor de actieve centrale. Voor redundante centrales moet de firmware-installatie worden uitgevoerd voor beide centrales. Hiertoe moeten de rollen van de twee centrales worden omgewisseld, en na een geslaagde installatie van de firmware weer worden hersteld door ze opnieuw om te wisselen.

Opmerking!
Firmwareversies
Voor een systeem dat uitsluitend AVENAR-knooppunten bevat, wordt aanbevolen om het te laten draaien op de nieuwste centralefirmwareversie 4.x.
Voor een systeem dat ten minste één FPA/FMR-knooppunt bevat, wordt aanbevolen om het te laten draaien op de nieuwste centralefirmwareversie 3.x.

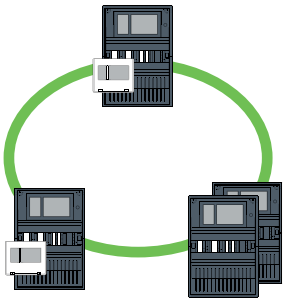
Opmerking!
Van 1 januari 2022 tot 31 december 2025 bevindt centralefirmwareversie 3.x zich in de onderhoudsmodus. Gedurende deze periode zullen nieuwe versies worden uitgebracht met oplossingen voor kritieke bugs en kritieke beveiligingslacunes. Er zijn geen nieuwe productkenmerken, LSN-randapparatuur, GUI-talen en normatieve wijzigingen gepland om te worden toegevoegd.
Na 31 december 2025 nemen beveiligingsrisico's toe op centrales die zijn aangesloten op een Ethernet-interface of -netwerk en draaien op firmware V3.x. Het wordt sterk aanbevolen om een beveiligingsrisicobeoordeling uit te voeren. Wanneer beveiligingsrisico's worden geïdentificeerd, is het verplicht om te upgraden naar een AVENAR panel en deze te laten draaien op de nieuwste firmware V4.x.

Opmerking!
Redundante paneelcontroller
Een paneelcontroller van de AVENAR panel-serie en een paneelcontroller van de FPA-serie kunnen niet worden gecombineerd voor redundantie.

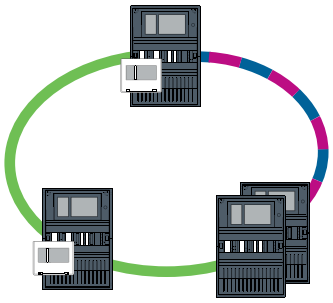
4 Topologieën

In dit document worden uiteenlopende netwerktopologieën voor brandalarmen beschreven. De topologieën worden onafhankelijk van het type brandmeldcentrale beschreven.

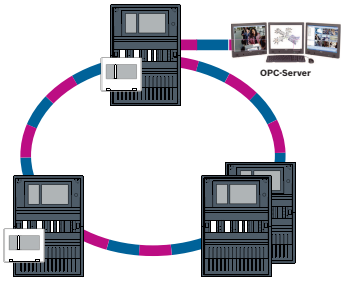
Opmerking!
Toepasselijke topologieën
De functionaliteit en de communicatie tussen centrales worden beperkt door het centraletype. Raadpleeg de specificaties van de centrale voor informatie over services, het aantal centrales dat kan worden aangesloten en het aantal externe bedieningspanelen dat kan worden aangesloten.



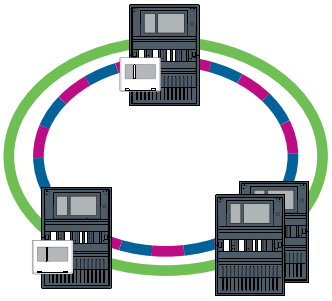
CAN-lus, pagina 16



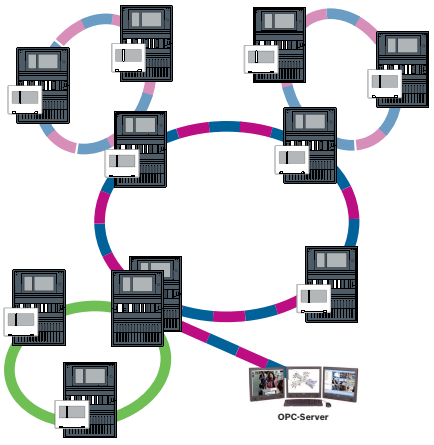
CAN-lus met Ethernet-segmenten, pagina 18



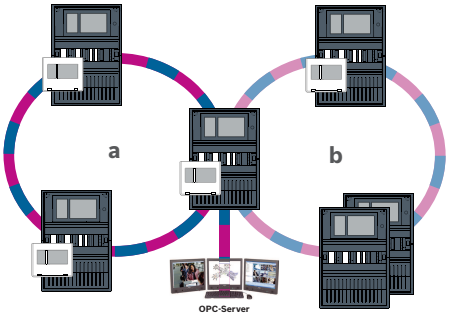
Ethernet-lus, pagina 17
Ethernet-lus met OPC-server, pagina 17
Ethernet-lus met OPC-server naar redundante centrale, pagina 18



Dubbele Ethernet-/CAN-lus, pagina 18

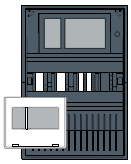
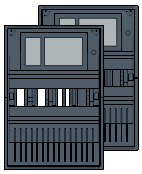
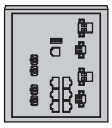


Ethernet-backbone met sublussen (Ethernet/CAN), pagina 18



Verbonden Ethernet-lussen, pagina 20

Kabel	Omschrijving
	TX Ethernet-kabel (koper), TX-kabellengte van knooppunt tot knooppunt < 100 m
	FX Ethernet-kabel (glasvezelkabel)
	TX of FX Ethernet-kabel, TX-kabellengte van knooppunt tot knooppunt < 100 m
	CAN-kabel, CAN-kabellengte van knooppunt tot knooppunt < 1000 m

Apparaat	Omschrijving
	Centrale of extern bedieningspaneel (in Ethernet-topologie elk een interne RSTP-switch)
	Centrale of redundante centrale (in Ethernet-topologie interne RSTP-switch) Een extern bedieningspaneel kan worden gebruikt als redundante paneelcontroller. Voor een redundante paneelcontroller en een redundant bedieningspaneel gelden identieke netwerkverbindingen en instellingen. Gebruik van een redundant bedieningspaneel is alleen van toepassing voor AVENAR panel 8000.
	Ethernet-switch als externe RSTP-switch (in het algemeen Ethernet-switch MM)
	Mediaconverter
	Beveiligde netwerkgateway voor Remote Services

Limieten in een netwerk

Het aantal centrales en externe bedieningspanelen dat kan worden verbonden in een netwerk, is afhankelijk van de gekozen netwerktopologie.

Centrales en externe bedieningspanelen in een netwerk worden knooppunten genoemd.

- Het aantal detectiepunten in een netwerk is beperkt tot 32768.
- Het aantal detectiepunten per centrale die werkt in een netwerk, is beperkt tot 2048.
- Het aantal knooppunten per systeem is afhankelijk van het type topologie.
  Een knooppunt is een paneelcontroller of een extern bedieningspaneel.
- Het aantal knooppunten in een lustopologie is beperkt tot 32.
- Met FSP-5000-RPS kunt u maximaal 3 geconfigureerde externe bedieningspanelen toewijzen aan één centrale.

De bekabeling tussen knooppunten en de maximaal toegestane kabellengte wordt ook bepaald door de gekozen topologie.

Maximaal 32 paneelcontrollers, externe bedieningspanelen en OPC-servers kunnen worden gecombineerd in een netwerk.

Afhankelijk van de gewenste toepassing kunnen verschillende paneelcontrollers en externe bedieningspanelen in groepen worden ingedeeld en worden gedefinieerd als netwerkknooppunten of lokale knooppunten. In de regel kan in elke groep alleen de status van centrales in de gedefinieerde groep worden weergegeven. De status van alle centrales kan worden weergegeven en/of verwerkt vanuit netwerkknooppunten, onafhankelijk van de groep waartoe de centrales behoren.

Fysiek knooppuntadres

Een centrale of extern bedieningspaneel wordt aangeduid in het netwerk met een uniek adres, ook wel het fysieke knooppuntadres genoemd.

Opmerking!
Fysiek knooppuntadres voor redundante centrales
Een redundante centrale moet hetzelfde fysieke knooppuntadres hebben als de toegewezen primaire centrale.

Opmerking!
Het gebruikte netwerk moet voldoen aan de volgende minimale vereisten:
Minimale doorvoer: 1 Mbps
Maximale vertraging: 250 ms

Opmerking!
EN 54
Gebruik alleen onderdelen die zijn goedgekeurd voor gebruik in centrale brandalarmnetwerken, om er zeker van te zijn dat het netwerk voldoet aan EN 54.
Externe RSTP-switches en media-omvormers in Ethernet-netwerken moeten worden geïnstalleerd in behuizingen van centrales. Installaties buiten de centralebehuizing voldoen niet aan EN 54.

Opmerking!
Redundante centrale - EN 54-2
Voor elke centrale kunnen maximaal 512 detectiepunten worden verbonden volgens EN 54-2. Als dit aantal wordt overschreden, moet de centrale met redundantie worden ontworpen. Ook moet de centrale als redundant worden ontworpen als deze fungeert als interface met een CAN-sublus en er meer dan 512 detectiepunten zijn verbonden in de sublus. De RSTP-switch die 2 lussen verbindt, biedt de redundantie.
Voor een zelfstandige centrale kunnen 4096 detectiepunten worden verbonden, zelfs als de centrale met redundantie is ontworpen. Als de centrale is opgenomen in een netwerk, kunt u maximaal 2048 detectiepunten aansluiten.

Opmerking!
Zorg dat het fysieke knooppuntadres dat aan de centrale is toegewezen, overeenkomt met het nummer in de programmeersoftware. De laatstgenoemde is verantwoordelijk voor het instellen van het laatste nummer van het IP-adres in de standaardinstellingen.
Activeer RSTP als redundantieprotocol en gebruik de standaardwaarden.

Standaard Ethernet-instellingen van brandmeldcentrale
In de standaardinstellingen van de brandmeldcentrale gebruiken zowel de programmeersoftware FSP-5000-RPS als de regeleenheid het ingestelde fysieke knooppuntadres als het laatste nummer van het IP-adres.

Opmerking!
Op de paneelcontrollers en in de programmeersoftware FSP-5000-RPS is een juiste instelling van het fysieke knooppuntadres vereist voor een werkzaam netwerk.

Opmerking!
Gebruik van de Ethernet-redundantie moet afzonderlijk worden geactiveerd in de paneelcontroller.

– IP-instellingen

  - IP-adres 192.168.1.x
    Het laatste cijfer van het IP-adres in de standaardinstellingen is altijd gelijk aan het fysieke knooppuntadres dat is ingesteld op de paneelcontroller.
  - Netwerkmasker 255.255.255.0
  - Gateway 192.168.1.254
  - Multicast-adres 239.192.0.1
  - Poortnummer 25001 - 25008 (alleen de eerste poort kan worden ingesteld, er worden altijd 8 opeenvolgende poorten gebruikt)
- RSTP-parameters (standaardinstellingen)
  - Bridge Priority 32768
  - Hello Time 2
  - Max. Age 20
  - Forward Delay 15

Opmerking!
U kunt de standaardinstellingen van de IP-configuratie gebruiken voor netwerken met maximaal 20 RSTP-switches.
Voor netwerken met meer dan 20 RSTP-switches zijn aanvullende instellingen vereist op basis van de topologie. Hiervoor is uitgebreide kennis van netwerken vereist.

Instellingen voor lussen met meer dan 20 RSTP-switches
Als er meer dan 20 RSTP-switches aanwezig zijn in het netwerk, moet u de RSTP -instellingen aanpassen op de paneelcontroller en in de programmeersoftware. Paneelcontrollers, externe bedieningspanelen en de verbonden externe RSTP-switches worden beschouwd als RSTP-switches. Redundante paneelcontrollers worden niet beschouwd als RSTP-switches, omdat de hierin opgenomen switch niet werkt als een RSTP-switch.

- RSTP-parameters
  - Houd Bridge Priority 32768 ongewijzigd
  - Houd Hello Time 2 ongewijzigd
  - Wijzig Max. Age van 20 in 40
  - Wijzig Forward Delay van 15 in 25

Parameters

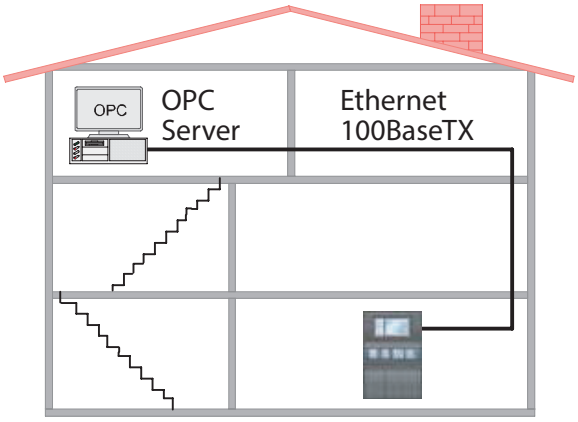
- In een lus kunnen maximaal 32 knooppunten worden gebruikt.
- De diameter van het netwerk mag niet groter zijn dan 32, zie *Netwerkdiameter, pagina 23*.
- Ethernet-switches mogen niet worden gebruikt buiten centralebehuizingen.
- Media-omvormers mogen niet worden gebruikt buiten centralebehuizingen.

Productkenmerken

- Het netwerk voldoet aan EN 54.
- Het netwerk maakt gebruik van RSTP.

Verbinding met BIS met OPC-server
Bij verbindingen met een gebouwbeheersysteem (BIS) via een OPC-server en Ethernet 100BaseTX in meerdere netwerken, moet u bij de netwerkbeheerder controleren of:

1. Het netwerk is ontworpen voor meerdere gebouwverbindingen (bijvoorbeeld, er mag geen technische interferentie zijn door potentiaalverschillen in aarding).
2. De bandbreedte van de busgebruikers voldoende is voor het netwerk.



Afbeelding 4.1: Verbinding met BIS via OPC-server

Aanvullende informatie bij gebruik van een OPC-server

OPC-servers in uw netwerk moeten worden toegevoegd aan de programmeersoftware FSP-5000-RPS.

U moet de volgende instellingen gebruiken in de FSP-5000-RPS-software en op de OPC-server:

- Netwerkknooppunten
- Netwerkgroep
- RSN
- IP-adres
- Poort

De OPC-server maakt standaard gebruik van poort 25000.

Opmerking!

EN 54

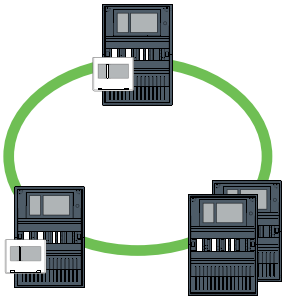
De aansluiting van een gebouwbeheersysteem (bijv. BIS) via een Ethernet-interface met gebruikmaking van een OPC-server of een FSI-server is conform EN54 als de functies die relevant zijn voor EN54, alleen door de brandmeldcentrale worden uitgevoerd. Voor elke besturings- of beheerfunctie met EN54-relevantie (bijv. de besturing van signaleringsapparaten of het beheer van uitschakeling) door het gebouwbeheersysteem is een afzonderlijke EN54-certificering van het algehele systeem door een certificeringsinstantie vereist.

Opmerking!

De programmeersoftware FSP-5000-RPS

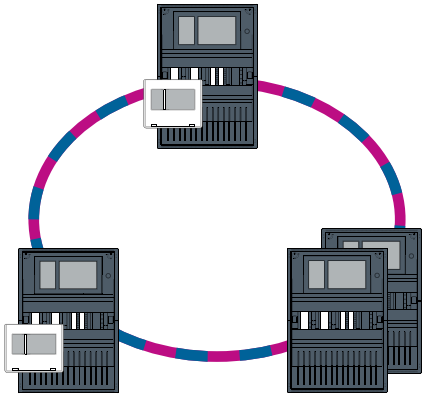
U moet een OPC-server toewijzen aan elk netwerkknooppunt waarvan de status moet worden verzonden.

4.1 CAN-lus



Afbeelding 4.2: CAN-lus

4.2 Ethernet-lus



Afbeelding 4.3: Ethernet-lus

4.3 Ethernet-lus met OPC-server

De Ethernet-switch voor het verbinden van de OPC-server moet afzonderlijk worden geprogrammeerd

Programmeer het IP-adres en de redundantie-instellingen van de Ethernet-switch, zie *Instellingen op switch , pagina 51*. Omdat de switch in de onmiddellijke nabijheid (zonder tussenruimte) wordt geïnstalleerd, hoeft de voeding niet te worden ontworpen als redundant en worden de storingsuitgangen daarom niet gebruikt.

Zorg dat de RSTP-instellingen in de paneelcontrollers, de FSP-5000-RPS en de Ethernet-switch identiek zijn.

De OPC-server moet afzonderlijk worden geprogrammeerd

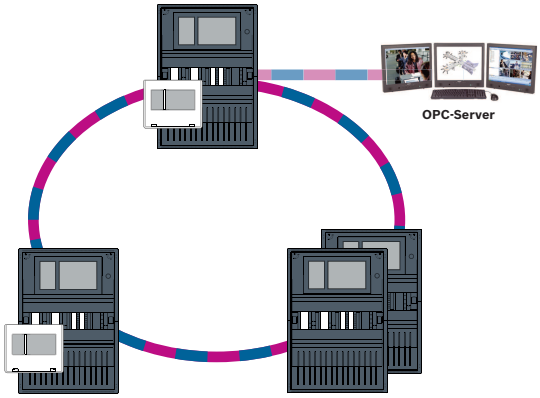
Programmeer het IP-adres, de netwerkknooppunten, de netwerkgroep en het RSN. Zie het desbetreffende gedeelte in het hoofdstuk Installatie van de Netwerkhandleiding.

De OPC-server maakt standaard gebruik van poort 25000.

Zorg dat de instellingen in de programmeersoftware FSP-5000-RPS en de OPC-server identiek zijn.

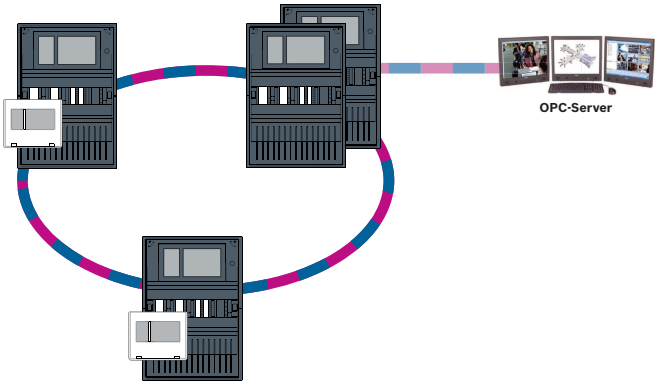
Parameters

– De OPC-server kan worden verbonden via een Ethernet-kabel (koper) of glasvezelkabel.



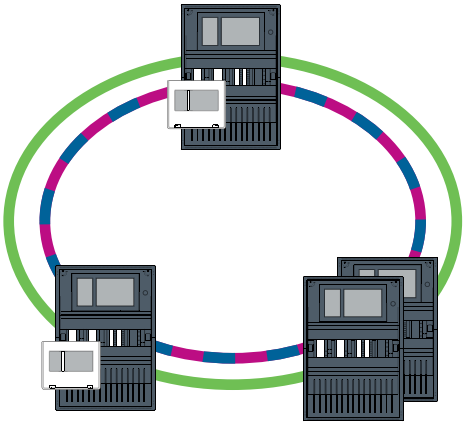
Afbeelding 4.4: Ethernet-lus met OPC-server

4.4 Ethernet-lus met OPC-server naar redundante centrale



Afbeelding 4.5: Ethernet-lus met OPC-server naar redundante centrale

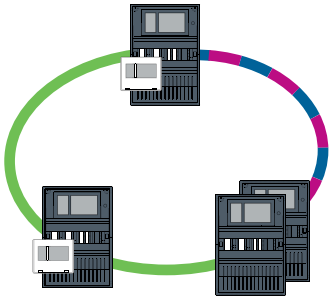
4.5 Dubbele Ethernet-/CAN-lus



Afbeelding 4.6: Dubbele lus van Ethernet en CAN

4.6 CAN-lus met Ethernet-segmenten

De hoofdtopologie is een CAN-lus. Wanneer de afstand tussen twee knooppunten groter is dan 1000 m, kan een FX Ethernet-verbinding worden gebruikt om de afstand te overbruggen.



Afbeelding 4.7: CAN-lus met Ethernet-segmenten

4.7 Ethernet-backbone met sublussen (Ethernet/CAN)

Een Ethernet-backbone is verbonden met alle sublussen, voor een kernverbindingsgebied met een hoge gegevenstransmissiesnelheid. Standaard zijn de RSTP-switches in de backbone niet superieur aan de andere RSTP-switches. Let erop dat u met deze topologie de netwerkdiameter moet bepalen. Paneelcontrollers, externe bedieningspanelen en de verbonden externe RSTP-switches worden beschouwd als RSTP-switches. In een CAN-netwerk opgenomen centrales worden buiten beschouwing gelaten bij het bepalen van de netwerkdiameter.

Houd rekening met de instellingen voor lussen met meer dan 20 RSTP-switches, zie *Instellingen voor lussen met meer dan 20 RSTP-switches, pagina 15*.

Opmerking!
Voor deze topologie zijn aanvullende instellingen vereist voor alle RSTP-switches in de backbone. Daarom is meer gedetailleerde kennis van netwerken vereist.

Opmerking!
Als de centrale optreedt als een interface met een CAN-sublus, moet deze centrale volgens EN 54-2 ook als redundant worden ontworpen als er meer dan 512 detectiepunten zijn verbonden in de sublus.
Deze beperking geldt niet in een Ethernet-sublus, omdat de switches die de twee lussen verbinden voor de redundantie zorgen.

Aanvullende instellingen
De centrale lus moet werken als de backbone. Deze centrale lus moet via Ethernet met het netwerk zijn verbonden.

Opmerking!
Stel voor alle RSTP-switches in de backbone een hogere RSTP-prioriteit in dan in de sublussen. Zo weet u zeker dat de RSTP-hoofdbrug altijd in de backbone blijft, zelfs in geval van een storing.
De RSTP-switches voor het verbinden van de lussen maken deel uit van de backbone!
Gebruik een RSTP-prioriteit van 16384 in de backbone.

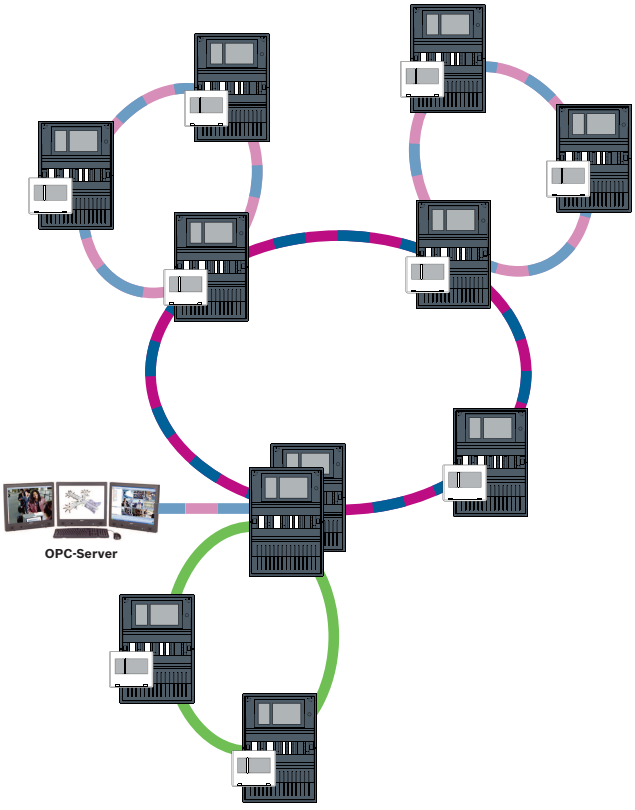
Opmerking!
Een lagere ingestelde waarde geeft een hogere RSTP-prioriteit aan.

De switches voor het verbinden van de OPC-server en de sublussen moeten afzonderlijk worden geprogrammeerd
Programmeer het IP-adres en de redundantie-instellingen van de Ethernet-switches, zie *Instellingen op switch , pagina 51*. Voor deze topologie moeten de storingsuitgangen van de switch alleen worden gebruikt als u de voeding voor de switch als redundant hebt ontworpen of als er een verbinding van switch naar switch is, zie *Ethernet-switch, pagina 62*.
Zorg dat de RSTP-instellingen in de paneelcontrollers, de FSP-5000-RPS en de Ethernet-switch identiek zijn.

Opmerking!
Wijzig de RSTP-prioriteit voor de RSTP-switches voor het verbinden van de lussen, aangezien deze tot de backbone behoren.

De OPC-server moet afzonderlijk worden geprogrammeerd.
Programeer het IP-adres, netwerkknooppunten, netwerkgroep en RSN, zie *OPC-servers, pagina 68*.
De OPC-server maakt standaard gebruik van poort 25000.
Zorg dat de instellingen in de RPS-programmeersoftware en de OPC-server identiek zijn.

Parameters
– De OPC-server kan worden verbonden via een Ethernet-kabel (koper) of glasvezelkabel.



Afbeelding 4.8: Ethernet-backbone met sublussen

4.8 Verbonden Ethernet-lussen

Opmerking!
Voor deze topologie zijn aanvullende instellingen vereist voor alle RSTP-switches in de backbone. Daarom is meer gedetailleerde kennis van netwerken vereist.

Aanvullende instellingen
Deze topologie is een speciaal exemplaar van de Ethernet-backbone met sublussen, zie Ethernet-backbone met sublussen (Ethernet/CAN). U moet een van de twee lussen laten werken als de backbone.

Opmerking!
Stel voor alle centrales en switches in de backbone een hogere RSTP-prioriteit in dan in de sublussen. Zo weet u zeker dat de RSTP-hoofdbrug altijd in de backbone blijft, zelfs in geval van een storing.
De switches voor het verbinden van de twee lussen maken deel uit van de backbone! Gebruik een RSTP-prioriteit van 16384 in de backbone.

Opmerking!
Een lagere ingestelde waarde geeft een hogere RSTP-prioriteit aan.

De switches voor het verbinden van de OPC-server en de tweede lus moeten afzonderlijk worden geprogrammeerd

Programmeer het IP-adres en de redundantie-instellingen van de Ethernet-switch, zie *Instellingen op switch , pagina 51*. Voor deze topologie moeten de storingsuitgangen van de switch alleen worden gebruikt als u de voeding voor de switch als redundant hebt ontworpen, zie *Ethernet-switch, pagina 62*.

Zorg dat de RSTP-instellingen in de paneelcontrollers, de FSP-5000-RPS en de Ethernet-switch identiek zijn.

Wijzig de RSTP-prioriteit voor de switches voor het verbinden van de twee lussen, aangezien deze tot de backbone behoren.

De OPC-server moet afzonderlijk worden geprogrammeerd

Programmeer het IP-adres, de netwerkknooppunten, de netwerkgroep en het RSN. Zie het desbetreffende gedeelte in het hoofdstuk Installatie van de Netwerkhandleiding.

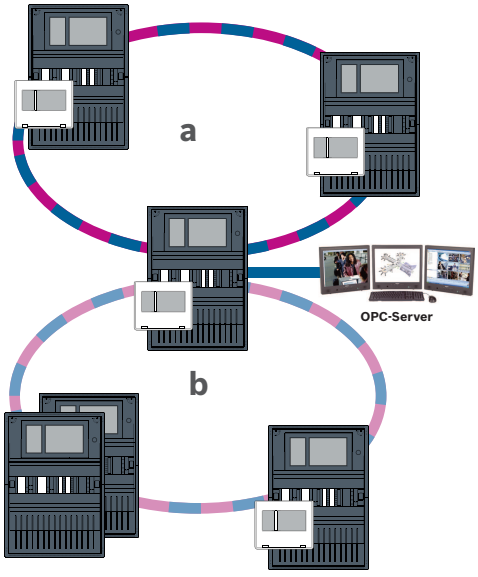
De OPC-server maakt standaard gebruik van poort 25000.

Zorg dat de instellingen in de programmeersoftware FSP-5000-RPS en de OPC-server identiek zijn.

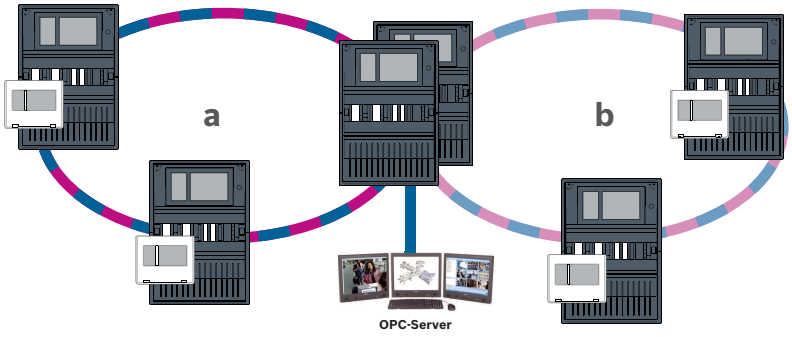
Parameters

– De OPC-server kan worden verbonden via een Ethernet-kabel (koper) of glasvezelkabel.

In deze voorbeelden is lus a de backbone. Lus b is de sublus.



Afbeelding 4.9: Ethernet-lus die is verbonden via een niet-redundante centrale



Afbeelding 4.10: Ethernet-lus die is verbonden via een redundante centrale

5 Ethernet-netwerk

De Ethernet-verbindingen in het netwerk worden voortdurend bewaakt. Als een verbinding is verbroken, wordt de onderbreking gedetecteerd. Gerepareerde verbindingen worden ook gedetecteerd. De netwerkdiagnose van de centrale geeft altijd het MAC-adres weer van de hosts die zijn verbonden via het netwerk.

MAC-adressen

Elke paneelcontroller verstrekt de volgende MAC-adressen voor de netwerkverbinding.

– MAC-adres voor de host
– MAC-adres ter identificatie van de ETH1-poort
– MAC-adres ter identificatie van de ETH2-poort

Afhankelijk van het type paneelcontroller:

– MAC-adres ter identificatie van de ETH3-poort
– MAC-adres ter identificatie van de ETH4-poort

Regels voor het gebruik van 4 Ethernet-poorten

Als uw centrale 4 Ethernet-poorten heeft, past u de volgende regels in de vermelde volgorde toe. Bosch ondersteunt enkel netwerken die zijn samengesteld volgens de volgende regels.

1. Voor centralenetwerken moeten ETH1 en ETH2 worden gebruikt. Voor centralenetwerken dient uitsluitend een externe RSTP-switch op ETH1 of ETH2 te worden gebruikt.
2. Voor het aansluiten van een OPC, een FSM-5000-FSI, een gesproken woord ontruimingssysteem en een UGM-2040 moet u ETH3 gebruiken. U mag een externe RSTP-switch aansluiten, die echter niet mag worden gebruikt voor centralenetwerken.
3. Voor Remote Services moet u ETH4 gebruiken. Als geen aansluiting op Remote Services vereist is, kan ETH4 worden gebruikt voor het aansluiten van een OPC, een FSM-5000-FSI, een gesproken woord ontruimingssysteem of een UGM-2040.
4. Als er geen centralenetwerk wordt gebruikt via ETH1 en ETH2, kan elk hiervan worden gebruikt voor het aansluiten van een OPC, een FSM-5000-FSI, een gesproken woord ontruimingssysteem of een UGM-2040.

5.1 Protocollen

SNMP

SNMP wordt gebruikt om netwerkonderdelen te bewaken en te beheren. Parameters van netwerkknooppunten kunnen daarvoor worden gelezen of gewijzigd. Hiervoor is de juiste netwerkbeheersoftware vereist (bijvoorbeeld Hirschmann HiVision).

Opmerking!

Het netwerk gebruikt de vaste SNMP-communitytekenreeks: PUBLIC

Houd er rekening mee dat de AVENAR panel-serie nog geen ondersteuning biedt voor het SNMP-protocol.

LLDP

LLDP is een basisprotocol dat is gestandaardiseerd door de IEEE en wordt gebruikt om netwerkinformatie tussen aangrenzende apparaten te delen. Deze informatie wordt

– verstrekt als onderdeel van de SNMP-gegevens en
– weergegeven via de paneelcontroller als onderdeel van de diagnostische netwerkgegevens.

RSTP

RSTP is een netwerkprotocol dat is gestandaardiseerd door de IEEE. RSTP zorgt ervoor dat er geen lussen aanwezig zijn in netwerken. Redundante paden in het netwerk worden gedetecteerd, gedeactiveerd en geactiveerd wanneer dat nodig is (storing van een verbinding). Het protocol wordt exact hiervoor gebruikt in het netwerk.
Een wijziging in de topologie na een storing van een verbinding wordt automatisch geannuleerd zodra deze is gerepareerd.

5.2 Netwerkdiameter

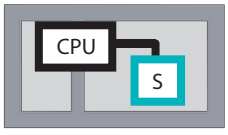
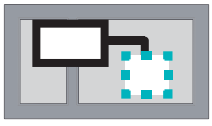
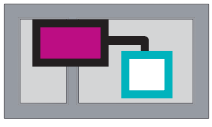
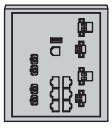
De netwerkdiameter van RSTP Ethernet-netwerken van centrales mag niet groter zijn dan 32.

Definitie

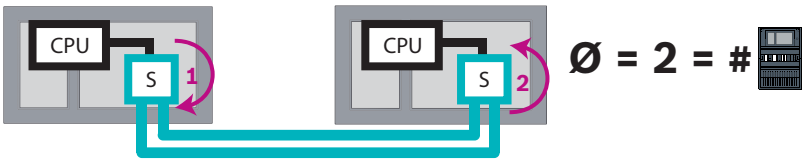
De diameter van een netwerk komt overeen met het aantal RSTP-switches op de langst mogelijke sectie zonder lussen tussen 2 eindpunten in het netwerk.
Bij een RSTP Ethernet-centralenetwerk moet u rekening houden met het volgende:

- Elke paneelcontroller bevat een eindpunt en een interne RSTP-switch.
- Een combinatie van een paneelcontroller en een redundante paneelcontroller telt als slechts één RSTP-switch.
- Media-omvormers worden niet beschouwd als RSTP-switch.
- CAN-verbindingen mogen niet worden opgenomen in de langst mogelijke sectie.
- Bij het bepalen van de diameter worden OPC-servers buiten beschouwing gelaten.

Legenda

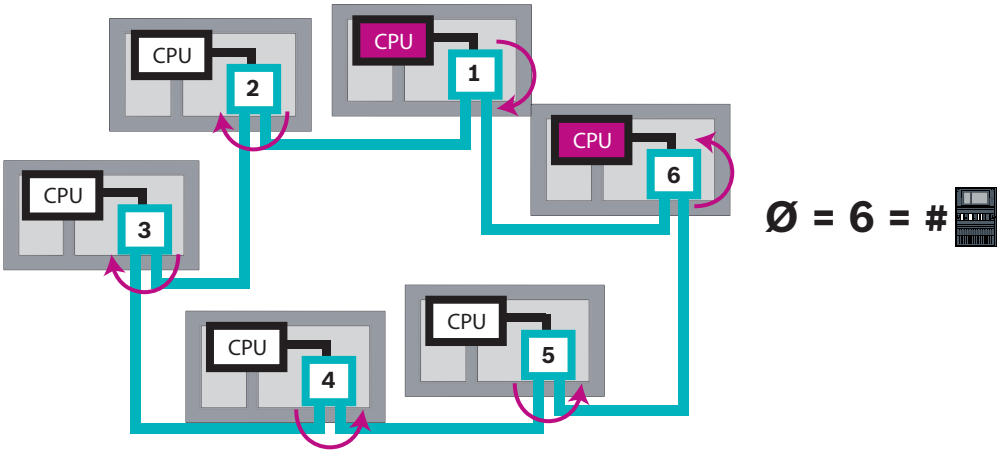
	Centrale processor in de paneelcontroller of het externe bedieningspaneel.
	Interne RSTP-switch in de paneelcontroller of in het externe bedieningspaneel.
	Paneelcontroller of extern bedieningspaneel met centrale processor en interne RSTP-switch.
	Redundante paneelcontroller met centrale processor en interne RSTP-switch.
	Paneelcontroller of extern bedieningspaneel Begin- of eindpunt voor het bepalen van de netwerkdiameter in de voorbeelden.
	Ethernet-switch als externe RSTP-switch (in het algemeen Ethernet-switch MM)

2 verbonden centrales vormen de kleinst mogelijke lus. De diameter van dit netwerk is 2, omdat de interne RSTP-switches zich bevinden tussen de eindpunten.



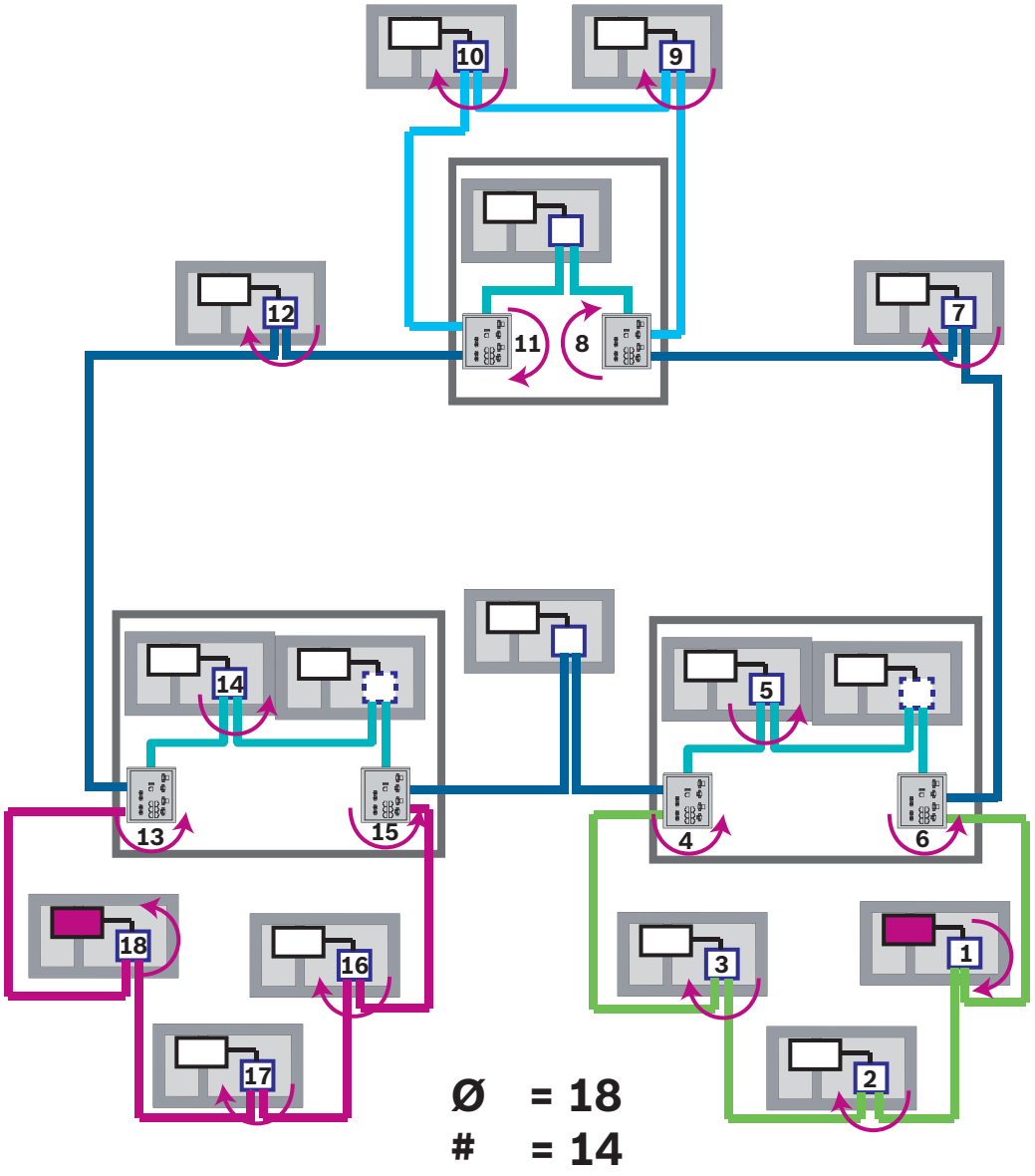
Afbeelding 5.1: Netwerkdiameter van een lus met 2 centrales

In een centralelus zonder externe RSTP-switches komt de diameter van het netwerk overeen met het aantal geïnstalleerde centrales.



Afbeelding 5.2: Netwerkdiameter van een lus met 6 centrales

Als een backbone en sublussen met elkaar zijn verbonden via Ethernet-switches, moet er ook rekening worden gehouden met deze externe RSTP-switches.



Afbeelding 5.3: Netwerkdiameter van een backbone met sublussen

Zoals u ziet in de afbeelding, wordt de diameter bepaald aan de hand van het langste pad.

5.3 Gebruikte kabels

Gebruik alleen de volgende kabels voor het netwerk. Het gebruik van andere kabels is niet conform de veiligheidsnormen in de EG-richtlijnen.

- Ethernet-kabel
  Ethernet-patchkabel, afgeschermd, CAT 5e of beter.
  Let op de minimale buigradius in de kabelspecificatie.
- Glasvezelkabel
  Multimode: glasvezel Ethernet-patchkabel, duplex I-VH2G 50/125µ of duplex I-VH2G 62.5/125µ, SC-stekker.
  Single-mode: glasvezel Ethernet-patchkabel, duplex I-VH2E 9/125µ, SC-stekker.
  Let op de minimale buigradius in de kabelspecificatie.

Opmerking!
TX-kabellengte
Alle IP-verbindingen moeten direct zijn of via media-omvormers die zijn goedgekeurd door Bosch. De TX-kabellengte van knooppunt tot knooppunt moet minder zijn dan 100 m.

Opmerking!
VdS 2540
Gebruik glasvezelkabel voor Ethernet-verbindingen om te voldoen aan de vereisten van VdS 2540 voor gegevenstransmissiekanalen. Voor verbindingen binnen een behuizing kunnen TX Ethernet-kabels worden gebruikt.

5.4 Een Ethernet-netwerk maken of wijzigen

Er zijn meerdere procedures voor het maken van een Ethernet-netwerk van brandmeldcentrales. Het verschil tussen de 2 procedures die hieronder worden beschreven, wordt bepaald door de grootte van het netwerk en het aantal installatie- en configuratietaken dat gelijktijdig moet worden uitgevoerd.

Regels voor het gebruik van 4 Ethernet-poorten

Als uw centrale 4 Ethernet-poorten heeft, past u de volgende regels in de vermelde volgorde toe. Bosch ondersteunt enkel netwerken die zijn samengesteld volgens de volgende regels.

1. Voor centralenetwerken moeten ETH1 en ETH2 worden gebruikt. Voor centralenetwerken dient uitsluitend een externe RSTP-switch op ETH1 of ETH2 te worden gebruikt.
2. Voor het aansluiten van een OPC, een FSM-5000-FSI, een gesproken woord ontruimingssysteem en een UGM-2040 moet u ETH3 gebruiken. U mag een externe RSTP-switch aansluiten, die echter niet mag worden gebruikt voor centralenetwerken.
3. Voor Remote Services moet u ETH4 gebruiken. Als geen aansluiting op Remote Services vereist is, kan ETH4 worden gebruikt voor het aansluiten van een OPC, een FSM-5000-FSI, een gesproken woord ontruimingssysteem of een UGM-2040.
4. Als er geen centralenetwerk wordt gebruikt via ETH1 en ETH2, kan elk hiervan worden gebruikt voor het aansluiten van een OPC, een FSM-5000-FSI, een gesproken woord ontruimingssysteem of een UGM-2040.

Een Ethernet-netwerk maken (kleinere projecten)

Deze procedure is geschikt voor projecten waarbij een klein aantal technici gelijktijdig aan de installatie van het brandalarmsysteem werkt.

1. Plan het netwerk.
2. Maak het netwerk in FSP-5000-RPS en configureer de netwerkinstellingen.
3. Druk de netwerkinformatie af om deze te bewaren of sla de informatie op de laptop op.
4. Installeer de centrales en de netwerkkabels en verbind ze met een netwerk.
5. Configureer de netwerkinstellingen voor de afzonderlijke centrales rechtstreeks op het bedieningspaneel, zoals in het afgedrukte document.
6. Reset elke centrale in het netwerk om de netwerkconfiguratie te activeren.
7. Verbind uw computer waarop de programmeersoftware FSP-5000-RPS is geïnstalleerd, met een centrale in het netwerk. Laad deze configuratie via deze centrale naar alle centrales in het netwerk. Redundante centrales gebruiken de configuratie van de hoofdcentrale.
8. Voer een reset uit om de foutmeldingen te resetten. Corrigeer alle fouten.

Configureer eerst de netwerkinstellingen op de centrales. U hebt dan het voordeel dat u de andere centrales in het netwerk kunt programmeren vanaf één centrale.

Een Ethernet-netwerk maken (middelgrote en grote projecten)

Deze procedure is geschikt voor projecten waarbij meerdere taken gelijktijdig moeten worden uitgevoerd door meerdere teams. Omdat bij veel taken tijdens de installatie en configuratie de brandmeldcentrale opnieuw moet worden opgestart, wordt het netwerk pas opgestart in een later stadium.

1. Plan het netwerk.
2. Maak een configuratie van het netwerk zonder randapparatuur met FSP-5000-RPS.
3. Druk de netwerkinformatie af om deze te bewaren of sla de informatie op de laptop op.
4. Installeer de netwerkkabels en controleer de afzonderlijke secties of lussen.
5. Installeer de centrales en neem ze in gebruik als zelfstandige centrales.
6. Installeer de randapparatuur in de centrales.
7. Configureer elke centrale met FSP-5000-RPS.
8. Controleer of de afzonderlijke centrales correct werken.
9. Neem de afzonderlijke lussen van het netwerk één voor één in gebruik volgens de topologie.

   Begin met de backbone.
   - Maak een configuratie voor de backbone in FSP-5000-RPS. Importeer alle benodigde centraleconfiguraties. Configureer de netwerkinstellingen en druk deze af.
   - Verbind alle centrales met een netwerk.
   - Configureer de netwerkinstellingen voor de afzonderlijke centrales rechtstreeks op de paneelcontroller, zoals in het afgedrukte document.
   - Reset elke centrale om de netwerkconfiguratie te laden.
   - Ping de aangrenzende centrales om het netwerk te controleren.
   - Neem de hele backbone in gebruik en corrigeer eventuele fouten.

   Neem de sublussen in gebruik zoals in het voorbeeld van de backbone.

Een centrale toevoegen aan een netwerk

1. Wijzig de netwerkconfiguratie in FSP-5000-RPS.
2. Druk de netwerkinformatie af om deze te bewaren of sla de informatie op de laptop op.
3. Installeer de centrale en de netwerkkabels en verbind ze met het netwerk.
4. Configureer de netwerkinstellingen voor de afzonderlijke centrale rechtstreeks op de paneelcontroller, zoals in het afgedrukte document.
5. Reset de centrale en aangrenzende centrales om de netwerkconfiguratie te activeren.

Een centrale verwijderen uit het netwerk

1. Wijzig de netwerkconfiguratie in FSP-5000-RPS.
2. Druk de netwerkinformatie af om deze te bewaren of sla de informatie op de laptop op.
3. Configureer de netwerkinstellingen voor de aangrenzende centrales rechtstreeks op de paneelcontroller, zoals in het afgedrukte document.
4. Schakel de centrale uit, en schakel de voeding (netstroom en accu) uit voordat u de centrale uit het netwerk verwijdert.
5. Reset de aangrenzende centrales om de netwerkconfiguratie te activeren.

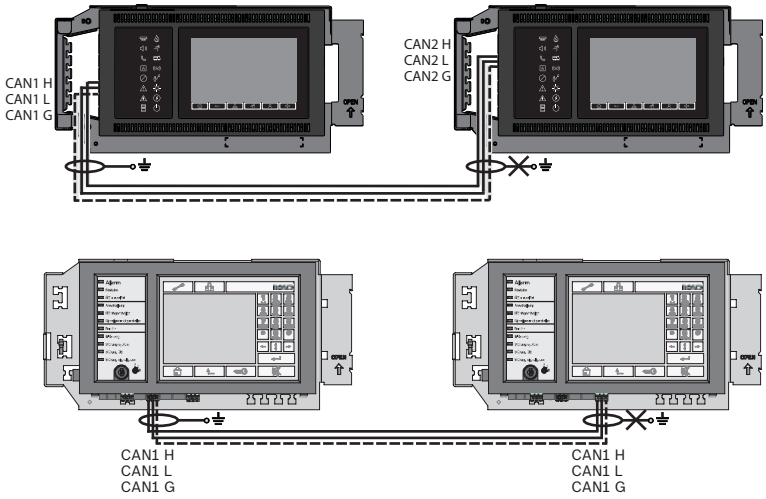
6 CAN-netwerk

Lustopologie

In een lustopologie wordt de CAN-kabel altijd omgeleid van een CAN1-aansluiting naar een CAN2-aansluiting [CAN1 ⇒ CAN2]. De kabellengte is afhankelijk van de dwarsdoorsnede van de kabel.

CAN-verbinding

De CAN-verbinding is een tweedraads verbinding (CAN-H en CAN-L). Verbind CAN-H met CAN-H en verbind CAN-L met CAN-L voor een tweedraads verbinding. In uitzonderlijke gevallen kan een driedraads verbinding (CAN-H, CAN-L en CAN-GND) nodig zijn, bijvoorbeeld bij een hoge EMC-belasting of een aanzienlijk potentiaalverschil in aarding. Verbind CAN-H met CAN-H, CAN-L met CAN-L en CAN-GND met CAN-GND voor een driedraads verbinding. De afgeschermde draad van de CAN-kabel is slechts aan één kant verbonden met de metalen behuizing van de centrale.



Afbeelding 6.1: CAN-verbinding (boven: AVENAR, onder: FPA)

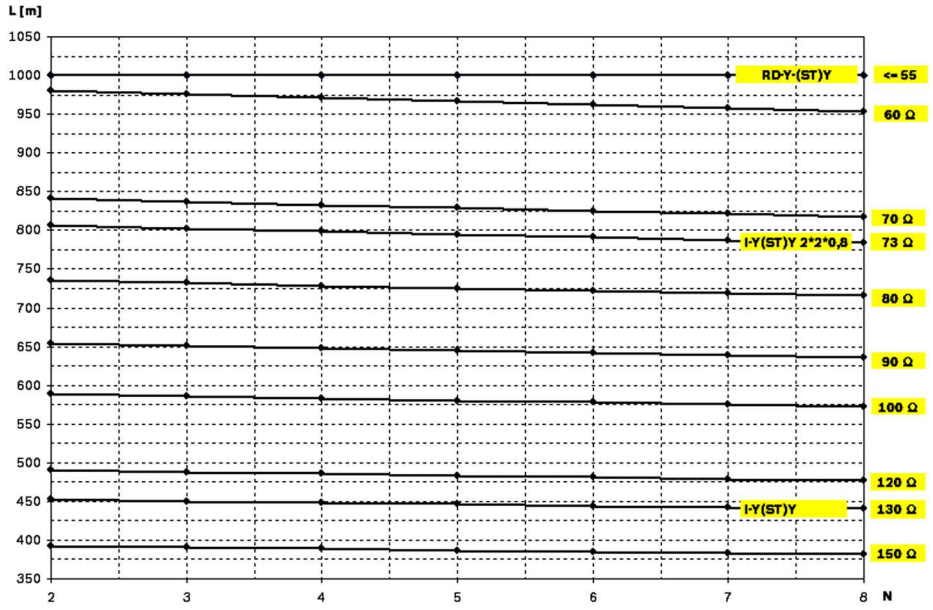
Kabellengte voor netwerken

De maximaal toegestane kabellengte is afhankelijk van de lusweerstand van de gebruikte kabel en van het aantal communicatieknooppunten.

Voorbeeld: de rode brandmelderkabel J-Y (St) Y 2 x 2 x 0,8 mm kan twee knooppunten met een maximale afstand van ongeveer 800 m met elkaar verbinden.

Opmerking!

De afstand tussen twee knooppunten in een lustopologie kan worden bepaald door de waarde bij de twee knooppunten in het diagram op te zoeken.



Afbeelding 6.2: CAN-netwerk: mogelijke kabellengte is afhankelijk van het aantal knooppunten en de kabelweerstand

L = kabellengte in meters

N = aantal knooppunten

6.1 Een CAN-netwerk maken of wijzigen

Deze procedure is geschikt voor projecten waarbij een klein aantal technici gelijktijdig aan de installatie van het brandalarmsysteem werkt.

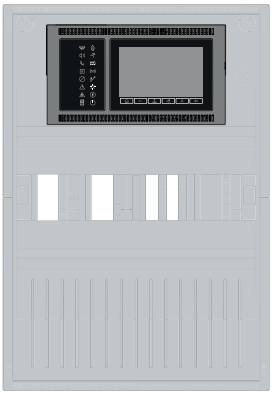
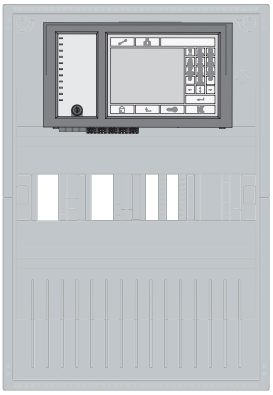
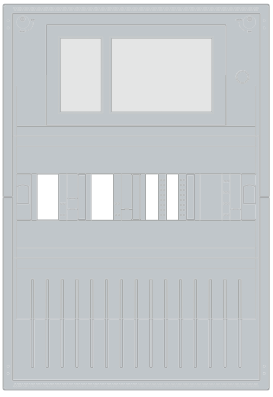
Procedure voor het maken van een CAN-netwerk

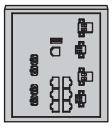
1. Plan het netwerk.
2. Maak het netwerk in FSP-5000-RPS.
3. Druk de netwerkinformatie af om deze te bewaren of sla de informatie op de laptop op.
4. Installeer de centrales en de verbind deze met CAN-kabels met een netwerk.
5. Verbind uw computer waarop de programmeersoftware FSP-5000-RPS is geïnstalleerd, met een centrale in het netwerk. Laad deze configuratie via deze centrale naar alle centrales in het netwerk. Redundante centrales gebruiken de configuratie van de hoofdcentrale.
6. Voer een reset uit om de foutmeldingen te resetten. Corrigeer alle fouten.

7 Ethernet- en CAN-netwerkpatroon

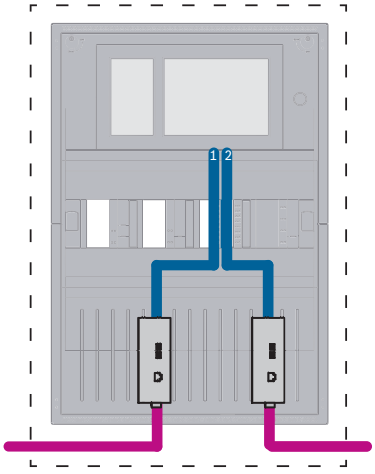
Voor het opbouwen van centralenetwerken overeenkomstig de geïntroduceerde topologieën en verbindingsservices, is het netwerkpatroon vereist dat in dit document wordt beschreven.

Pictogram	Omschrijving
	TX Ethernet-kabel (koper), TX-kabellengte van knooppunt tot knooppunt < 100 m
	FX Ethernet-kabel (glasvezelkabel)

Pictogram	Omschrijving
	TX of FX Ethernet-kabel, TX-kabellengte van knooppunt tot knooppunt < 100 m
	CAN-kabel
	Behuizing Opmerking: ter vereenvoudiging van het overzicht van verschillende netwerkpatronen wordt in de afbeeldingen in dit hoofdstuk altijd een kleine centralebehuizing weergegeven als symbool voor een centrale. Deze kleine behuizing biedt **niet** in alle vermelde gevallen voldoende ruimte voor de montage van de weergegeven switches, media-omvormers en gateways. Gebruik de Safety Systems Designer om te verzekeren dat u de juiste hoeveelheid en het juiste formaat behuizingen voor de installatie van de apparatuur bestelt.
	AVENAR panel
	FPA
	AVENAR panel of FPA

Pictogram	Omschrijving
	Ethernet-switch als externe RSTP-switch (in het algemeen Ethernet-switch MM)
	Mediaconverter
	Beveiligde netwerkgateway voor Remote Services
	Verbinding met OPC-server, FSM-5000-FSI, gesproken woord ontruimingssysteem of UGM-2040

7.1 Centralenetwerk via Ethernet



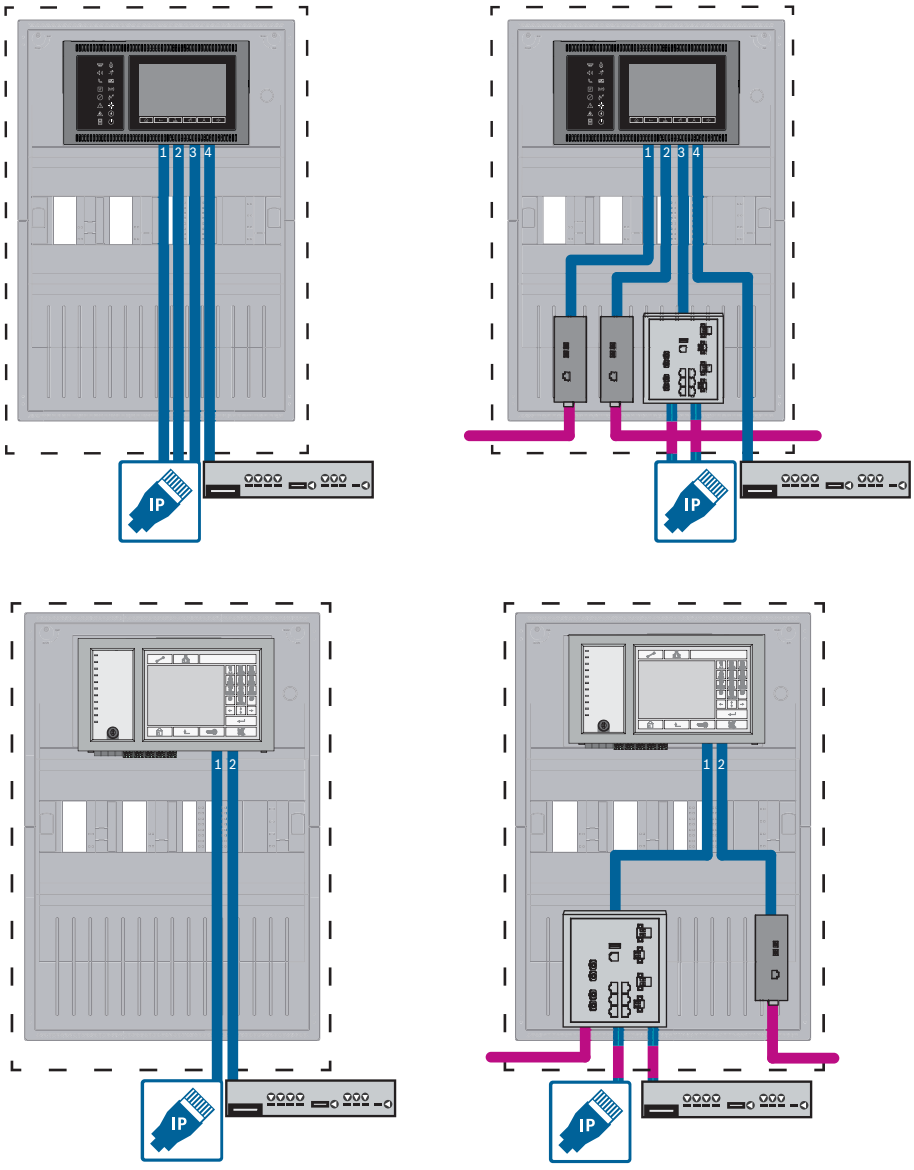
Afbeelding 7.1: Centralenetwerk via Ethernet

Voor een groter bereik dan 100 m is een uitbreiding van het bereik met media-omvormers verplicht. Voor een kleiner bereik dan 100 m is het gebruik van media-omvormers mogelijk niet vereist.

7.2 Centralenetwerk via CAN

Afbeelding 7.2: Centralenetwerk via CAN

7.3 Services aansluiten op centrale

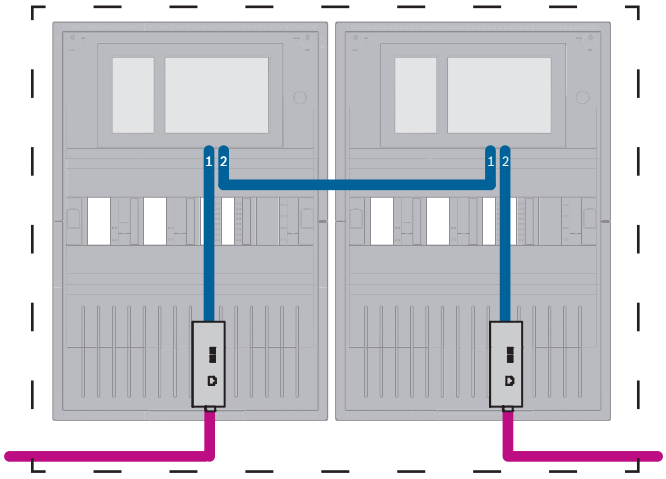


Afbeelding 7.3: Linkerzijde: zonder centralenetwerk, rechterzijde: met centralenetwerk

Alleen als meer dan twee services op de centrale zijn aangesloten, is de Ethernet-switch vereist.

Voor een groter bereik dan 100 m is een uitbreiding van het bereik met media-omvormers verplicht. Voor een kleiner bereik dan 100 m is het gebruik van media-omvormers mogelijk niet vereist.

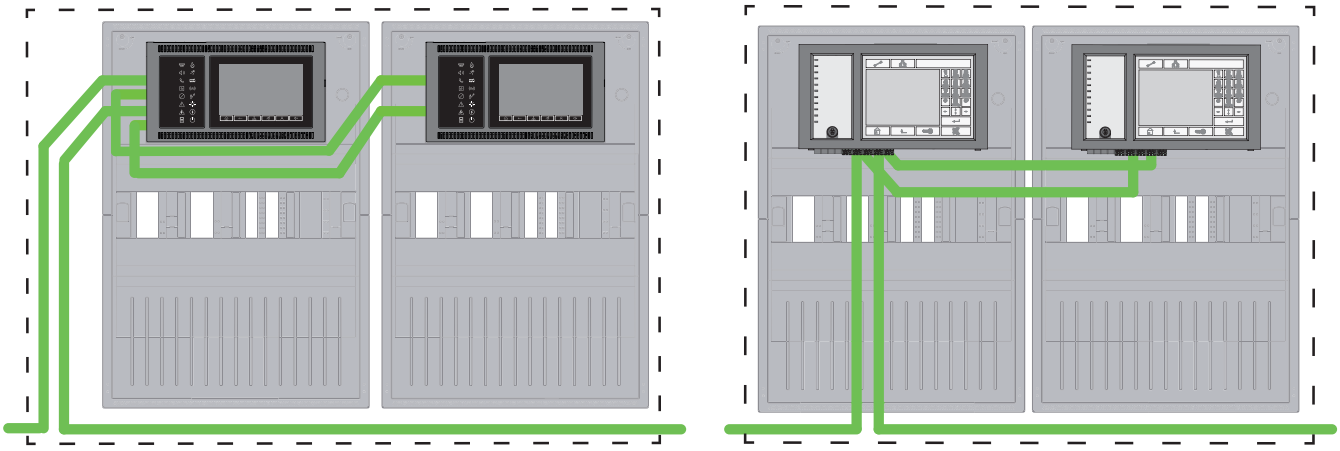
7.4 Centralenetwerk via Ethernet met redundante centrales



Afbeelding 7.4: Centralenetwerk via Ethernet met redundante centrales

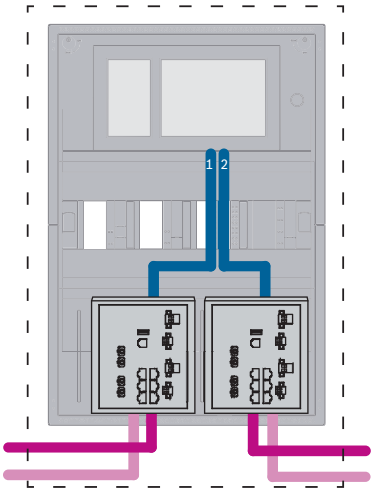
Voor een groter bereik dan 100 m is een uitbreiding van het bereik met media-omvormers verplicht. Voor een kleiner bereik dan 100 m is het gebruik van media-omvormers mogelijk niet vereist.

7.5 Centralenetwerk via CAN met redundante centrales



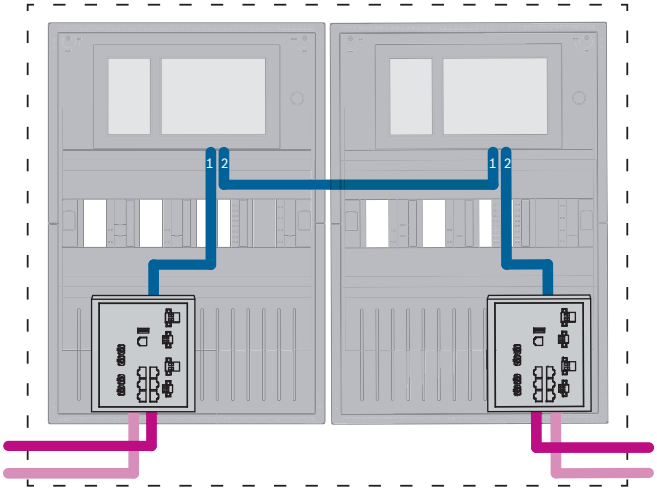
Afbeelding 7.5: Centralenetwerk via CAN met redundante centrales

7.6 Centralenetwerk via twee Ethernet-lussen



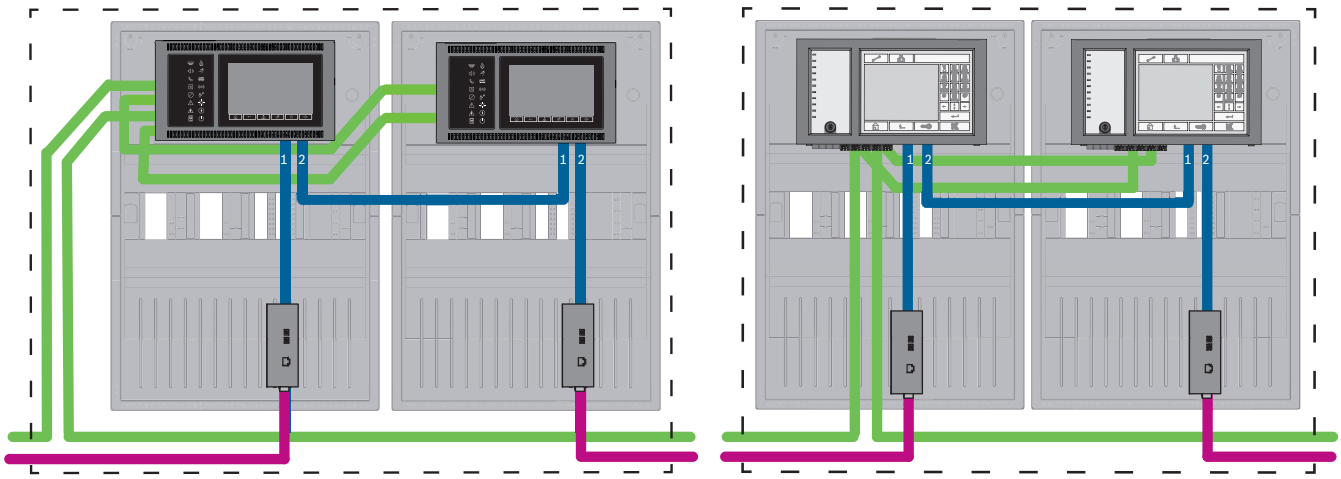
Afbeelding 7.6: Ethernet-netwerken verbinden

7.7 Centralenetwerk via twee Ethernet-lussen met redundante centrales



Afbeelding 7.7: Ethernet-netwerken met redundante centrales verbinden

7.8 Ethernet- en CAN-netwerken met redundante centrales verbinden



Afbeelding 7.8: Ethernet- en CAN-netwerken met redundante centrales verbinden

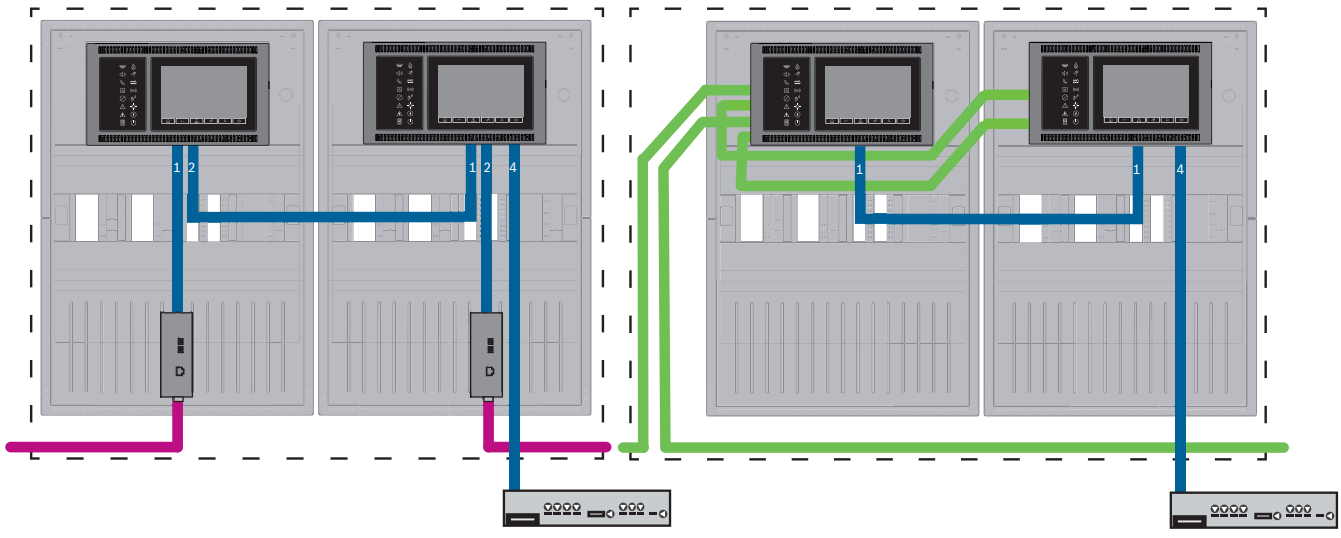
Voor een groter bereik dan 100 m is een uitbreiding van het bereik met media-omvormers verplicht. Voor een kleiner bereik dan 100 m is het gebruik van media-omvormers mogelijk niet vereist.

7.9 Remote Services verbinden met redundante centrales

Het is mogelijk om de beveiligde netwerkgateway aan te sluiten op een redundante FPA of op een redundante AVENAR panel. Overweeg om de volgende redenen om de beveiligde netwerkgateway niet aan te sluiten op een redundante AVENAR panel maar op een redundante AVENAR panel zonder centrale-redundantie:

- De procedure is een tussenoplossing.
- In geval van een aansluiting op een gebouwbeheersysteem via FSM-5000-FSI / OPC moet de ETH3-poort van de redundante paneelcontroller worden gebruikt en geconfigureerd.

7.9.1 Redundante AVENAR panel

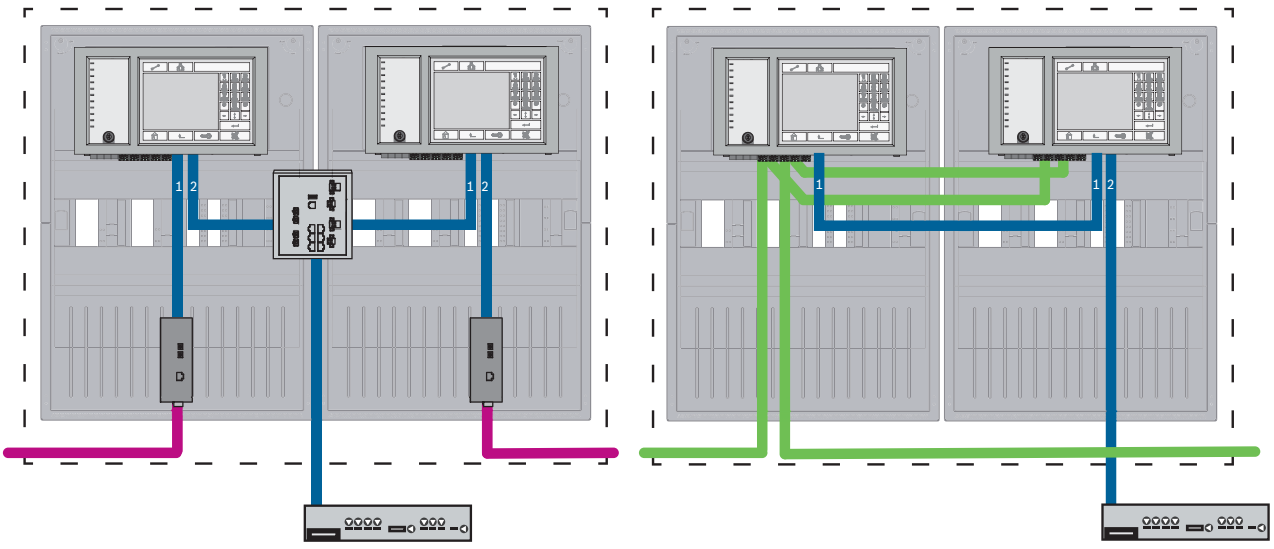


Afbeelding 7.9: Linkerzijde: in Ethernet-netwerk, rechterzijde: in CAN-netwerk

Voor een groter bereik dan 100 m is een uitbreiding van het bereik met media-omvormers verplicht. Voor een kleiner bereik dan 100 m is het gebruik van media-omvormers mogelijk niet vereist.

1. Voor het aansluiten van de beveiligde netwerkgateway sluit u deze aan op de ETH4-poort van de redundante paneelcontroller.
2. In het CAN-netwerk is een Ethernet-kabel vereist van de ETH1-poort naar de ETH1-poort van de redundante paneelcontroller. Configureer de ETH1-instellingen in het FSP-5000-RPS **Net-interface**-**Ethernet**-venster:
   - Voor **Lijntype** selecteert u **Link**
   - Een lijnnummer dat groter is dan 0 bij **Verbonden met lijnnummer**, zorgt ervoor dat de verbinding wordt bewaakt.
3. Of het nu gaat om een CAN-netwerk of een Ethernet-netwerk: voor beide configureert u de ETH4-instellingen in het FSP-5000-RPS **Net-interface**-**Ethernet**-venster:
   - Voer 0 in bij **Verbonden met lijnnummer**.
   - Markeer **Poort gebruiken**.

7.9.2 Redundante FPA



Afbeelding 7.10: Linkerzijde: in Ethernet-netwerk, rechterzijde: in CAN-netwerk

Voor een groter bereik dan 100 m is een uitbreiding van het bereik met media-omvormers verplicht. Voor een kleiner bereik dan 100 m is het gebruik van media-omvormers mogelijk niet vereist.

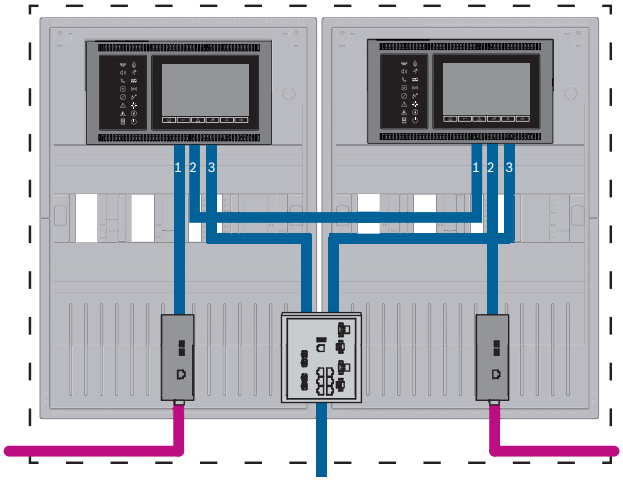
Procedure in CAN-netwerk

1. Voor het aansluiten van de beveiligde netwerkgateway sluit u deze aan op de ETH2-poort van de redundante paneelcontroller.
2. In het CAN-netwerk is een Ethernet-kabel vereist van de ETH1-poort naar de ETH1-poort van de redundante paneelcontroller. Configureer de ETH1-instellingen in het FSP-5000-RPS **Net-interface**-**Ethernet**-venster:
   - Voor **Lijntype** selecteert u **Link**
   - Een lijnnummer dat groter is dan 0 bij **Verbonden met lijnnummer**, zorgt ervoor dat de verbinding wordt bewaakt.
3. Configureer de ETH2-instellingen in het FSP-5000-RPS **Net-interface**-**Ethernet**-venster:
   - Voer 0 in bij **Verbonden met lijnnummer**.
   - Markeer **Poort gebruiken**.

7.10 Mogelijk mensenlevens reddende veiligheidsservices verbinden met redundante centrales

U moet mogelijk mensenlevens reddende veiligheidsservices verbinden met een redundante AVENAR panel zonder centrale-redundantie:

– De tussenoplossing voor Remote Services is niet geschikt voor mogelijk mensenlevens reddende, veiligheidsrelevante verbindingen met gesproken woord ontruimingssystemen (VAS over IP) of met een hiërarchiecentrale (UGM-2040). Er moet een EN 54-gecertificeerde switch worden geïnstalleerd die is aangesloten op de hoofdpaneelcontroller en op de redundante paneelcontroller.



Afbeelding 7.11: VAS- en hiërarchiecentrale-interface naar redundante AVENAR panel

8 Remote Services

De volgende services behoren tot Remote Services:

– Remote Connect
– Remote Alert
– Remote Maintenance

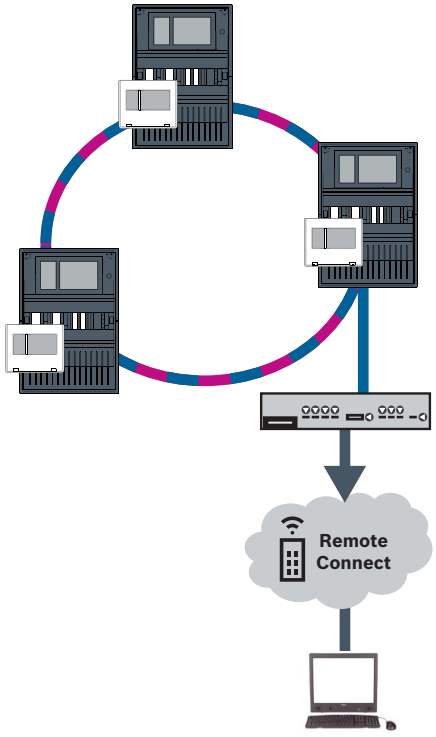
Voor Remote Alert en Remote Maintenance is Remote Connect vereist.

8.1 Remote Connect

Remote Connect biedt een vertrouwde en veilige internetverbinding voor externe toegang tot een centrale via FSP-5000-RPS. Remote Connect is de basis voor alle Remote Services. Gebruik de beveiligde netwerkgateway voor Remote Connect.
In het geval van een centralenetwerk moet één centrale in het centralenetwerk zijn verbonden met een beveiligde netwerkgateway. Uitsluitend deze verbinding moet een specifieke Ethernet-verbinding zijn.

Opmerking!
Remote Connect ondersteunt verbinding met een centralenetwerk via Ethernet of CAN. De functionaliteit van Remote Alert en Remote Maintenance wordt echter alleen ondersteund als er een Ethernet-netwerk tussen centrales aanwezig is en is geconfigureerd voor service.

Remote Connect moet worden ingeschakeld in de FSP-5000-RPS-configuratie van deze centrale.
In de volgende topologie ziet u paneelcontrollers die zijn verbonden via Ethernet, waarbij een beveiligde netwerkgateway is verbonden met het netwerk via een Ethernet-switch (in het algemeen MM).



Afbeelding 8.1: Remote Connect in een Ethernet-lus

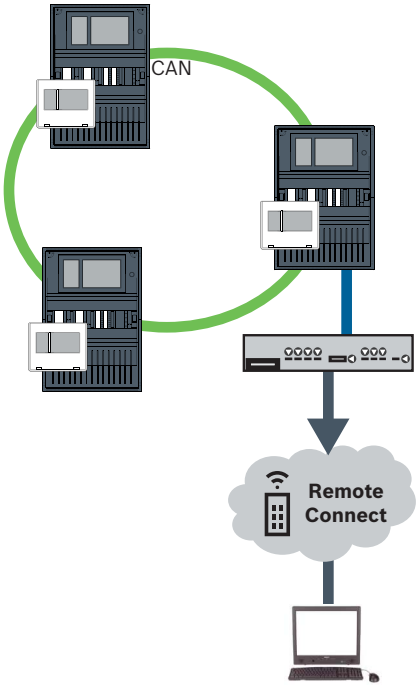
Opmerking!
Gebruik media-omvormers die zijn goedgekeurd door Bosch als u centrales wilt verbinden via FX.

Om te voorkomen dat multicast-verkeer dat relevant is voor EN 54-2 wordt verzonden naar de router, gebruikt u de Ethernet-switch (over het algemeen MM, BPA-ESWEX-RSR20) die is goedgekeurd met centraleversie 2.8. Activeer IGMP-snooping van de Ethernet-switch, zie het desbetreffende gedeelte in het hoofdstuk Installatie van de Netwerkhandleiding.

Opmerking!
De internetrouter (of het bedrijfsnetwerk dat internettoegang biedt) en de beveiligde netwerkgateway moeten gescheiden subnetwerken bieden. Centrales van het centralenetwerk mogen niet in het subnetwerk van de internetrouter worden geplaatst. Daarnaast is overlapping van de subnetwerken niet mogelijk.
Wanneer subnetwerken elkaar overlappen, moet u deze van elkaar scheiden door de IP-adressen aan de zijde van het centralenetwerk te wijzigen.
Daarnaast moet u de wijzigingen doorgeven aan de beveiligde netwerkgateway. Hiertoe opent u de webinterface via een webbrowser:
- Address (Adres): https://192.168.1.254
- User name (Gebruikersnaam): bosch
- Password (Wachtwoord): ipti83
Onder **Configuration (Configuratie)** -> **Network (LAN) [Netwerk (LAN)]** kunt u het IP-adres wijzigen. Denk eraan dat het adres bij **Standaard gateway:** in de configuratie van de paneelcontroller moet overeenkomen met het IP-adres van de beveiligde netwerkgateway.

Opmerking!
In overeenstemming met DIBt-richtlijnen is op afstand resetten via Remote Services om deursturingssystemen met gemotoriseerde openingsondersteuning weer gereed te maken voor bediening niet toegestaan.

In de volgende topologie ziet u een CAN-netwerk, waarbij een beveiligde netwerkgateway is verbonden met het netwerk via een Ethernet-poort.



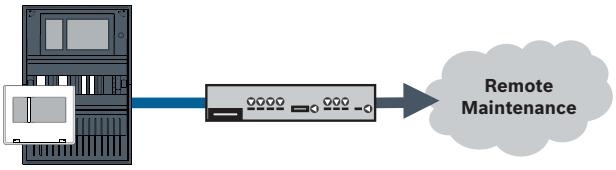
Afbeelding 8.2: Remote Connect in een CAN-lus

8.2 Remote Alert

Via Remote Alert verzendt een centrale relevante statusinformatie naar de Remote Portal.
De verzonden gegevens worden geanalyseerd met Remote Alert. In geval van een onverwachte gebeurtenis wordt de gebruiker via SMS en/of e-mail op de hoogte gebracht van de ontvangen waarschuwingen.
Remote Alert is tevens beschikbaar voor Private Secure Network.

8.3 Remote Maintenance

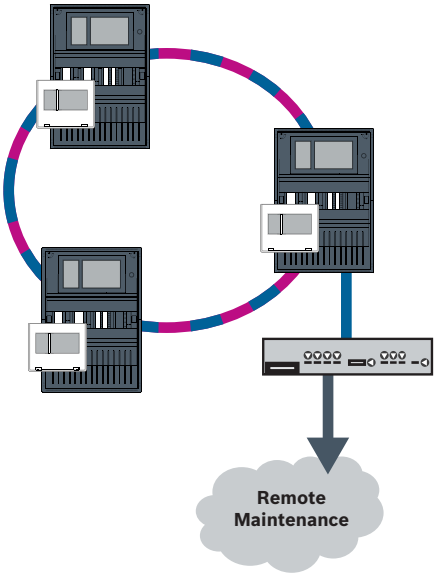
Remote Maintenance biedt de mogelijkheid voor bewaking op afstand van bepaalde parameters van diverse beveiligingsitems die zijn verbonden met een brandmeldcentrale. Via de Remote Portal kunt u looptests uitvoeren.



Afbeelding 8.3: Remote Maintenance

Opmerking!
Ethernet-verbindingen die alleen worden gebruikt voor het verzenden van Remote Maintenance-gegevens, kunnen zowel met Ethernet-kabels als glasvezelkabels tot stand worden gebracht. Let op de maximaal toegestane kabellengten.

Opmerking!
Gebruik media-omvormers die zijn goedgekeurd door Bosch als u centrales wilt verbinden via FX.



Afbeelding 8.4: Remote Maintenance

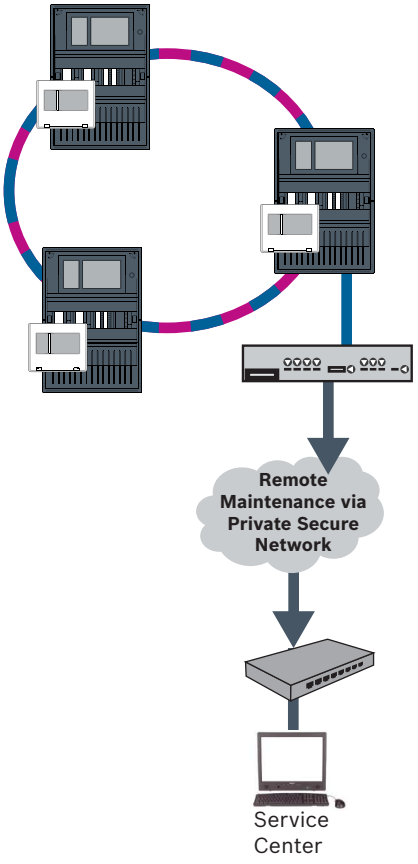
Bij gebruik van Remote Maintenance met Ethernet-netwerken moet één centrale in het netwerk met de router worden verbonden voor het verzenden van gegevens. Alle verzamelde gegevens worden vanuit het netwerk verzonden via deze verbinding.

Remote Maintenance voor Remote Portal
Remote Maintenance verzamelt gegevens van relevante LSN-apparaten en functionele modules en verzendt deze naar de Remote Portal waar ze worden geanalyseerd en weergegeven voor onderhoudsactiviteiten.

Remote Maintenance voor beveiligd privénetwerk
Remote Maintenance kan worden geconfigureerd voor een Private Secure Network: verzamelde gegevens worden verzonden naar een centraal managementserversysteem (CMS).

Voorzichtig!
Voor Remote Services is een beveiligde IP-verbinding vereist. Bosch Remote Services of een verbinding met Private Secure Network is vereist.
Bij gebruik van Private Secure Network hebt u de beschikking over een IP-netwerk dat is gebaseerd op DSL met optioneel draadloze toegang aan de kant van de centrale (EffiLink).
Remote Services voor Private Secure Network is alleen beschikbaar in Duitsland met een serviceovereenkomst met Bosch BT-IE.

Opmerking!
Gebruik media-omvormers die zijn goedgekeurd door Bosch als u centrales wilt verbinden via FX.



Afbeelding 8.5: Remote Maintenance voor beveiligd privénetwerk

Voor Remote Maintenance moet u het IP-adres van de server en de poort van de Remote Maintenance-systeemserver opgeven in de programmeersoftware FSP-5000-RPS.
Wijs een uniek centralenetwerk-ID toe aan het netwerk.

De switch voor het verbinden van de CMS moet afzonderlijk worden geprogrammeerd
Programmeer het IP-adres en de redundantie-instellingen van de switch, zie *Instellingen op switch , pagina 51*. Omdat de switch in de onmiddellijke nabijheid (zonder tussenruimte) wordt geïnstalleerd, hoeft de voeding niet te worden ontworpen als redundant en worden de storingsuitgangen daarom niet gebruikt.
Zorg dat de RSTP-instellingen in de paneelcontrollers, de FSP-5000-RPS en de Ethernet-switch identiek zijn.

8.4 Remote Portal

Vereisten

Opmerking!
Om herconfiguratie of aanpassingen bij het gebruik van Remote Services te voorkomen, moet aan de volgende vereisten worden voldaan:
- centrale met firmware 2.19.7 of hoger, alle centrales zijn verbonden via Ethernet, Ethernet-interfaces ingeschakeld en standaard Ethernet-instellingen
- Remote Connect ingeschakeld in de FSP-5000-RPS centraleconfiguratie
- Beveiligde netwerkgateway voor Remote Services beschikbaar
- computer waarop FSP-5000-RPS 4.8 of hoger is geïnstalleerd en met toegang tot internet

Opmerking!
Vermijd updates van de beveiligde netwerkgateway tijdens de verbinding.
Updates van de beveiligde netwerkgateway worden regelmatig uitgevoerd in de vroege ochtenduren. Geef daarom de tijdzone op onder **System** (Systeem) -> **General Settings** (Algemene instellingen) -> **Timezone** (Tijdzone).

Instructies
Voor het gebruik van Remote Services moet u een gebruiker van een Remote Portal-account zijn.

Stap 1: maak een Remote Portal-account
Onder één Remote Portal-account kunnen meerdere gebruikers worden gedefinieerd. Elk Remote Portal-account heeft één unieke Remote ID, die één bedrijf moet vertegenwoordigen. Als u geen bestaand Remote Portal-account kunt gebruiken, moet u er een maken:

1. Voer op https://remote.boschsecurity.com -> **Sign Up** (Aanmelden) uw naam, uw bedrijf en uw e-mailadres in en maak een wachtwoord. Neem de voorwaarden door en selecteer **I agree to the terms and conditions (Ik ga akkoord met de voorwaarden)**. Lees ook de privacyverklaring en selecteer **I agree to the privacy statement (Ik ga akkoord met de privacyverklaring)**.
2. Klik op **Register (Registreren)**.
   Het Remote Portal stuurt direct naar het opgegeven adres een e-mail met een activeringskoppeling.
3. Klik op de activeringskoppeling om het account te activeren. Klik in het Remote Portal op uw gebruikersnaam en selecteer **Account Settings (Accountinstellingen)**. Hier vindt u uw Remote ID. U hebt deze Remote ID later nodig op de paneelcontroller.

Als u al uw technici een eigen account wilt geven, kunt u voor dezelfde Remote ID verschillende gebruikers maken:
U wordt aangemeld bij het Remote Portal.

- Selecteer **Users** (Gebruikers) -> **New Technician** (Nieuwe technicus). Voer vervolgens de vereiste gegevens in en bevestig deze met **Save** (Opslaan).

Stap 2: verbind de beveiligde netwerkgateway
Gebruik een beveiligde netwerkgateway voor Remote Services.

1. Sluit de WAN-poort van de beveiligde netwerkgateway aan op de internetrouter of op het bedrijfsnetwerk dat internettoegang biedt.
2. Controleer op de internetrouter of het bedrijfsnetwerk de beschikbaarheid van de volgende protocollen en poorten voor de beveiligde netwerkgateway (vereist voor verbinding met Remote Services).

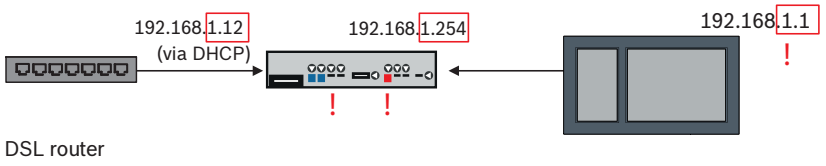
Protocol	Standaardpoort	Omschrijving
HTTP	80 en 8080	voor registratie van Remote Connect en Remote Maintenance
IPsec VPN	UDP 500 en UDP 4500	voor Remote Connect

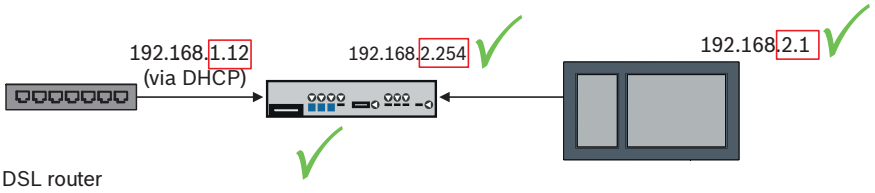
3. Sluit de LAN1-poort van de beveiligde netwerkgateway aan op de daarvoor bestemde Ethernet-poort van de paneelcontroller met gebruikmaking van de meegeleverde CAT5 RJ45-netwerkkabel. Let op de mogelijke topologieën.
4. Sluit de beveiligde netwerkgateway met gebruikmaking van de meegeleverde voeding aan op een netvoeding van 100 V - 230 V.

WAN-LED brandt (blauw) wanneer de verbinding met internet tot stand is gebracht. VPN-LED brandt (blauw) kort daarna, hetgeen betekent dat een VPN-verbinding met de Remote Portal tot stand is gebracht.
Elke aangesloten centrale of centralenetwerk heeft een unieke System ID.

Subnetwerken scheiden (VPN-LED uit)

De verbinding met de beveiligde netwerkgateway voor Remote Services mislukt als subnetwerken elkaar overlappen (VPN-LED uit). In het volgende voorbeeld ziet u een beveiligde netwerkgateway en een paneelcontroller in hetzelfde adresbereik als de DSL-router.





Een beveiligde netwerkgateway detecteert overlappende subnetwerken: de Alarm-LED knippert continu.
De subnetwerken worden gescheiden door het derde octet van het IP-adres te wijzigen. U wijzigt de IP-adressen aan de kant van het centralenetwerk. Nadat het IP-adres is gewijzigd, moet u de wijzigingen doorgeven aan de beveiligde netwerkgateway. Hiertoe opent u de webinterface via een webbrowser:
- Address (Adres): https://192.168.1.254
- User name (Gebruikersnaam): bosch
- Password (Wachtwoord): ipti83

Onder **Configuration (Configuratie)** -> **Network (LAN) [Netwerk (LAN)]** kunt u het IP-adres wijzigen. Denk eraan dat het adres bij **Standaard gateway:** in de configuratie van de paneelcontroller moet overeenkomen met het IP-adres van de beveiligde netwerkgateway.

Stap 3: breng een externe verbinding tot stand

1. Gebruik standaard Ethernet-instellingen bij de centrale.
2. Start de centrale opnieuw op.
3. Selecteer voor de verificatie **Configuration** (Configuratie) -> **Network Services** (Netwerkservices) -> **Change date / time** (Datum / tijd wijzigen), voer de huidige datum in en bevestig uw instellingen.
4. Selecteer **Configuration (Configuratie)** -> **Network Services (Netwerkservices)** -> **Remote Services** en voer de Remote ID in.

U kunt de status van de externe verbinding controleren: selecteer **Diagnostics (Diagnose)** -> **Network Services (Netwerkservices)** -> **Remote Services** bij de paneelcontroller.

Stap 4: wijs een licentie toe in de Remote Portal

Om het gebruik van de Remote Services te activeren, moet u een licentie toewijzen in de Remote Portal. Aan uw account wordt automatisch één licentie geleverd bij de eerste geslaagde verbinding.

Opmerking!
Een reeds toegewezen licentie kan niet opnieuw worden toegewezen of uitgesteld.

1. Voer op https://remote.boschsecurity.com -> **Login (Aanmelden)** uw e-mailadres en uw wachtwoord in.
2. Selecteer **Systems (Systemen)**.
3. Selecteer het systeem.
4. Klik onder **Services** op de knop **Add Service (Service toevoegen)** onder de service.
5. De licentie wordt standaard automatisch verlengd (**Service Settings (Service-instellingen)**, optie **With Auto-Renew (Automatisch verlengen)**).
6. Klik op **Save (Opslaan)** om uw instellingen te bevestigen.

Na het toewijzen van de licentie kunt u de bijbehorende service gebruiken. Een toegewezen licentie wordt aangeduid met een groene haak.

Stap 5: bestel licenties opnieuw

1. Bestel licenties voor één jaar bij Bosch branddetectiesystemen. Voor elk netwerk zijn specifieke licenties vereist.
   Bosch stuurt een e-mail naar het opgegeven adres. De e-mail bevat unieke licentieregistratienummers voor het aantal bestelde licenties, evenals instructies en een koppeling naar de Remote Portal.
2. Voer op https://remote.boschsecurity.com -> **Login** (Aanmelden) uw e-mailadres en uw wachtwoord in.
3. Selecteer **Licenses** (Licenties).
4. Klik op de knop **+**.
5. Volg de instructies in het venster **Add Licenses** (Licenties toevoegen) en bevestig met **Save** (Opslaan).
6. De lijst met licenties wordt bijgewerkt.

9 Smart Safety Link

Dit hoofdstuk specificeert de technische oplossing voor een veilige Ethernet-interface tussen Bosch-brandmeldcentrales (BMC's) en Bosch-systemen voor gesproken woord ontruiming.

Smart Safety Link is de meest betrouwbare en veilige interface om een branddetectiesysteem en een gesproken woord ontruimingssysteem (VAS) te combineren. Smart Safety Link biedt uitzonderlijke flexibiliteit en opties voor uitbreidbaarheid.
Een bewaakte verbinding tussen de brandmeldcentrale en het VAS wordt tot stand gebracht door bidirectionele gegevensuitwisseling. Zowel de brandmeldcentrale (BMC) als het VAS geven een storingsmelding aan wanneer de verbinding wordt onderbroken. In geval van een onderbroken verbinding kan de gebruiker de evacuatie van het volledige gebouw handmatig starten door gebruik te maken van een oproeppost van het VAS. Een onderbreking van de interface leidt niet tot een automatische ontruiming van het gebouw. Wanneer de interface opnieuw tot stand wordt gebracht, synchroniseert de brandmeldcentrale (BMC) automatisch de huidige alarmstatus opnieuw met het VAS. In geval van brand kan de brandmeldcentrale (BMC) automatisch gesproken aankondigingen starten door gebruik te maken van virtuele VAS-activeringen die worden geactiveerd door regels die zijn geconfigureerd in FSP-5000-RPS. De brandmeldcentrale (BMC) genereert een bewakingsmelding wanneer een evacuatiegebeurtenis wordt gestart vanuit het VAS. Een storing op het VAS zal een storingsmelding genereren op de gebruikersinterface van de brandmeldcentrale (BMC).
Via de grafische gebruikersinterface van een AVENAR panel heeft de operator de mogelijkheid om de aankondigingen van de brandmeldcentrale (BMC) te dempen. De operator kan een statusoverzicht van alle virtuele activeringen opvragen. Elke virtuele activering kan worden gemarkeerd met een ondubbelzinnig label met de locatie en het type melding. Een duidelijk onderscheidende kleur weerspiegelt de conditie van elke virtuele activering. Een operator met L2-gebruikersrechten kan de gesproken aankondiging in de geselecteerde virtuele activering handmatig starten en stoppen.
PAVIRO of Praesideo kan worden aangesloten op een FPA en AVENAR panel.
Vanwege de desbetreffende netwerktopologie vereist PRAESENSA een interface met gecodeerde gegevenscommunicatie. Gebruik alleen een AVENAR panel die draait op paneelcontrollerfirmwareversie 4.x om verbinding te maken met PRAESENSA.
Smart Safety Link over Ethernet werd geïntroduceerd in paneelcontrollerfirmwareversie 2.11 en FSP-5000-RPS versie 4.3.

Waarschuwing!
Ethernet-beveiligingsrisico's
Sluit PRAESENSA niet aan op FPA-5000/FPA-1200 met Smart Safety Link vanwege Ethernet-beveiligingsrisico's.

Opmerking!
Gesproken woord ontruimingssysteem aangesloten op AVENAR panel
Elke brandmeldcentrale (BMC) die via Smart Safety Link fysiek is aangesloten op een gesproken woord ontruimingssysteem, heeft een premium licentie nodig.

Opmerking!
Gesproken woord ontruimingssysteem aangesloten op FPA
Elke brandmeldcentrale (BMC) die via Smart Safety Link fysiek is aangesloten op een gesproken woord ontruimingssysteem en op firmwareversie 3.x draait, vereist geen licentiesleutel voor gesproken woord ontruiming.

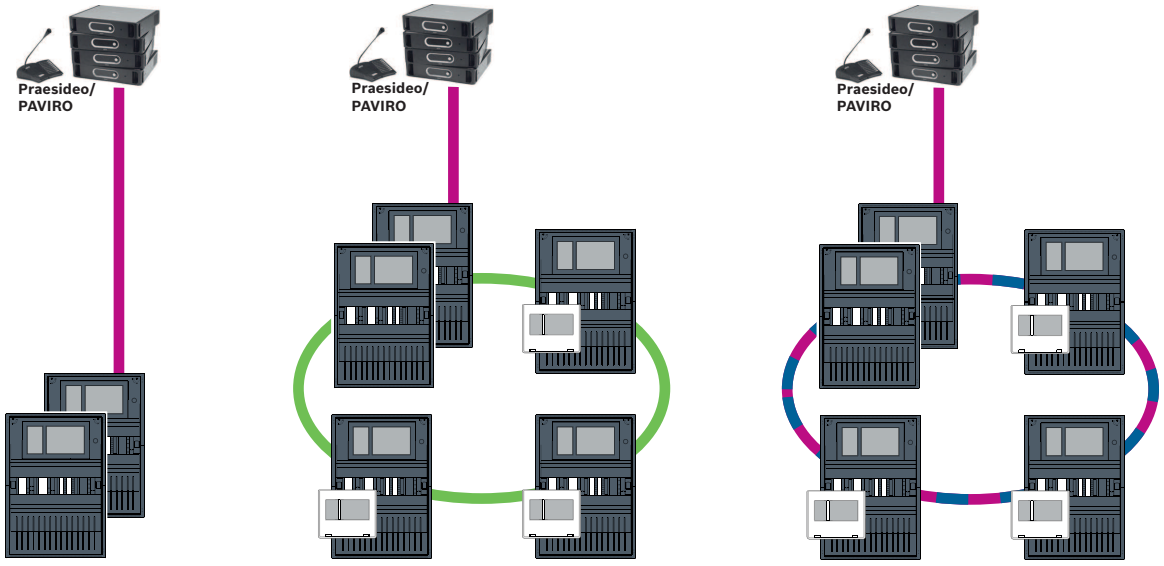
9.1 Eén directe VAS-interface

De brandmeldcentrale (BMC) en het gesproken woord ontruimingssysteem kunnen met één TX Ethernet-kabel worden aangesloten.

Opmerking!
VdS 2540
Het gesproken woord ontruimingssysteem moet samen (tegen elkaar) met de brandmeldcentrale (BMC) worden opgesteld in één en dezelfde ruimte. Anders wordt niet voldaan aan de vereisten van VdS 2540 voor gegevenstransmissiekanalen.

9.1.1 Praesideo en PAVIRO

AVENAR panel en FPA kunnen direct worden aangesloten op de speciale Open Interface Ethernet-poort van de systeemcontroller van Praesideo (PRS-NCO-3) of PAVIRO (PVA-4CR12). Gebruik de Open Interface voor één centrale of voor een centralenetwerk.

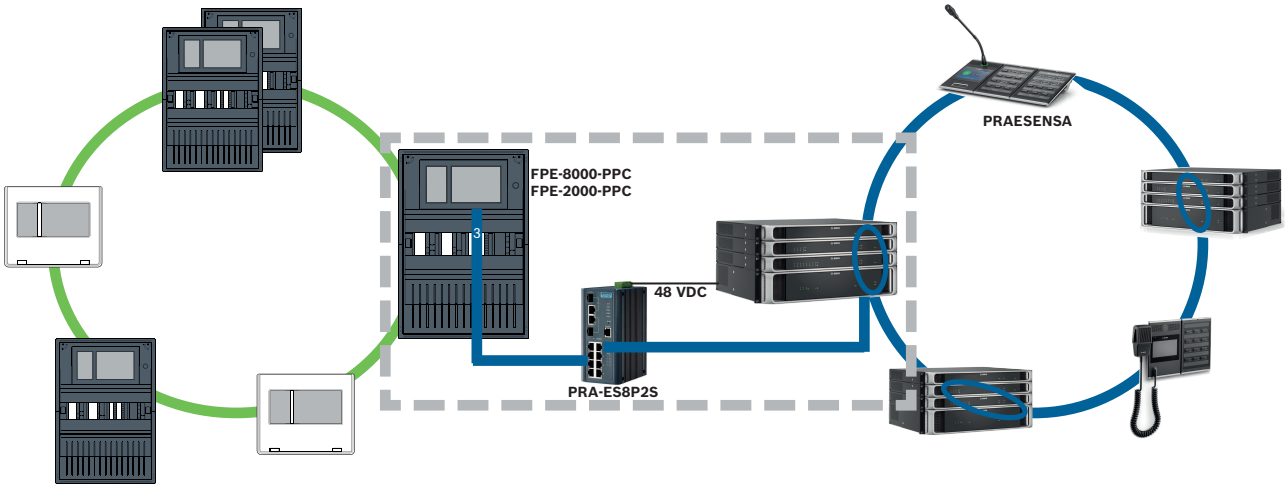


Afbeelding 9.1: Eén directe Praesideo|PAVIRO-interface

Opmerking!
Als een MPC-xxxx-B-paneelcontroller wordt gebruikt voor de directe verbinding met een Praesideo/PAVIRO-systeem, is een cross-over patchkabel vereist als de Praesideo/PAVIRO en de MPC-xxxx-B beide geen Auto-MDI(X) ondersteunen.

9.1.2 PRAESENSA

PRAESENSA is een in een netwerk te verbinden gesproken woord ontruimingssysteem dat gebruikmaakt van een IP-netwerk voor audio en regeling.
Sluit een AVENAR panel altijd via een PRA-ES8P2S Ethernet-switch, 8xPoE, 2xSFP aan op PRAESENSA.



Afbeelding 9.2: PRAESENSA naar AVENAR panel

Voorzichtig!
Ethernet-beveiligingsrisico's
Gebruik geen Smart Safety Link om PRAESENSA te verbinden met FPA-5000/FPA-1200. Gebruik alleen een AVENAR panel en AVENAR keypad 8000 in het volledige netwerk. Voor het aansluiten van PRAESENSA op FPA-5000/FPA-1200 gebruikt u relaiscontacten zoals gespecificeerd in TI2363/2021. Anders treden er Ethernet-beveiligingsrisico's op.

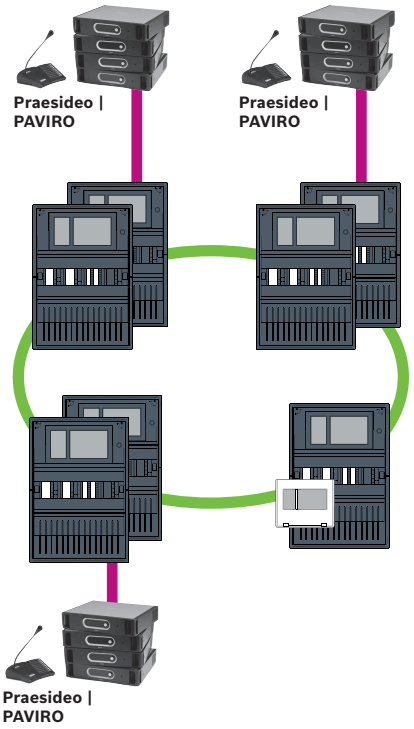
Opmerking!
PRAESENSA naar AVENAR panel
- Gebruik PRA-ES8P2S uitsluitend voor Smart Safety Link. Sluit naast de PRA-SCL-systeemcontroller geen andere PRAESENSA-apparatuur aan op de Ethernet-poorten van de Ethernet-switch, 8xPoE, 2xSFP. Gebruik de Ethernet-switch, 8xPoE, 2xSFP niet voor aansluiting op een gebouwbeheersysteem, hiërarchiecentrale, beveiligde netwerkgateway voor Remote Services enz.
- Gebruik een centrale met slechts één paneelcontroller om verbinding te maken met PRAESENSA door gebruik te maken van Smart Safety Link. Smart Safety Link naar PRAESENSA is nog niet compatibel met redundantie van de paneelcontroller. De centrales in het netwerk die niet rechtstreeks zijn aangesloten op PRAESENSA, kunnen redundantie van de paneelcontroller bevatten.
- Gebruik CAN-bustopologie voor het centralenetwerk. Gebruik geen Ethernet-centralenetwerk.
- Alle AVENAR panel-producten en alle AVENAR keypad 8000-producten in het netwerk moeten draaien op centralefirmware 4.x.

1. Monteer de PRA-ES8P2S Ethernet-switch in het PRAESENSA-rack. Installeer PRA-SCL in één lijn liggend met een AVENAR panel, in één en dezelfde ruimte. Monteer de PRA-ES8P2S Ethernet-switch niet in de AVENAR panel-behuizing.
2. PRAESENSA moet voorzien in de stroom voor PRA-ES8P2S.
3. Configureer de PRA-ES8P2S Ethernet-switch:
   - alleen unicast-communicatie tussen FPE-8000-PPC en PRAESENSA-controller toestaan
   - alle multicast-communicatie blokkeren
   - RSTP uitschakelen
4. Controleer de modus van PRAESENSA. Het moet in de modus DHCP worden uitgevoerd. De modus Zeroconf wordt niet ondersteund bij het gebruik van Smart Safety Link.

5. Sluit de PRAESENSA-controller aan via één Ethernet-kabel (RSTP uitgeschakeld).
6. Voor de Smart Safety Link-configuratie van AVENAR panel selecteert u **Encrypted VAS over IP (Gecodeerde VAS over IP)** in FSP-5000-RPS.

9.2 Meerdere directe VAS-interfaces

In een CAN-netwerk kan elke brandmeldcentrale (BMC) worden aangesloten op één gesproken woord ontruimingssysteem. Pas de directe interfaceaansluiting toe zoals gespecificeerd in *Eén directe VAS-interface, pagina 45*.



Afbeelding 9.3: Meerdere directe VAS-interfaces

Voor elk knooppunt waarvoor u het verbinden van een centrale in een netwerk via IP wilt deactiveren, voert u de volgende procedure uit in FSP-5000-RPS:

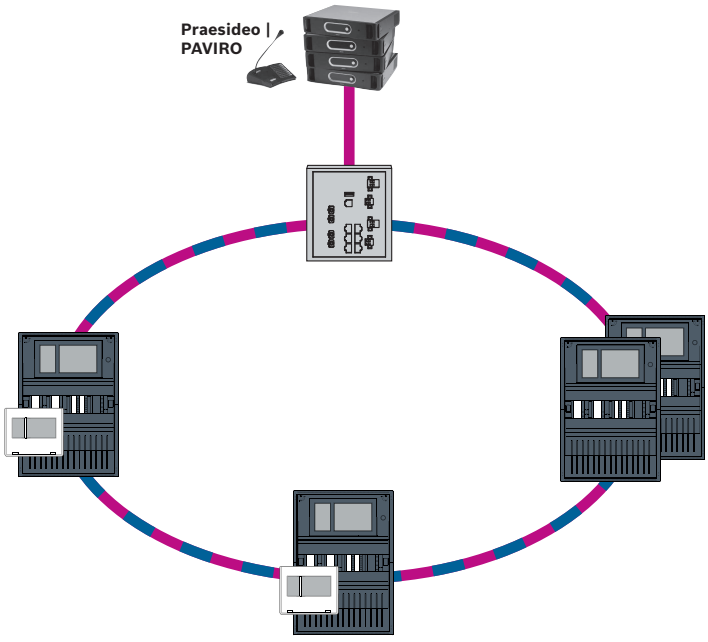
1. Selecteer het knooppunt voor het deactiveren van het verbinden van een centrale in een netwerk.
2. Selecteer **Ethernet-instellingen gebruiken**.
3. Deselecteer **Centralenetwerk via IP**.
4. Klik op **Toepassen**.

9.3 VAS geïntegreerd in Ethernet-centralenetwerk

Als Praesideo en PAVIRO zijn geïntegreerd in centralenetwerken, heeft het gesproken woord ontruimingssysteem een redundant transmissiekanaal. Het redundante transmissiekanaal maakt het mogelijk dat de brandmeldcentrale (BMC) en het gesproken woord ontruimingssysteem in aparte ruimtes worden geïnstalleerd.
Momenteel is het niet mogelijk om PRAESENSA te integreren in een Ethernet-centralenetwerk.

Opmerking!
VdS 2540
Het gesproken woord ontruimingssysteem moet samen (tegen elkaar) met de brandmeldcentrale (BMC) worden opgesteld in één en dezelfde ruimte. Anders wordt niet voldaan aan de vereisten van VdS 2540 voor gegevenstransmissiekanalen.

Opmerking!
VdS 2540
Gebruik glasvezelkabel voor Ethernet-verbindingen om te voldoen aan de vereisten van VdS 2540 voor gegevenstransmissiekanalen. Voor verbindingen binnen een behuizing kunnen TX Ethernet-kabels worden gebruikt.



Afbeelding 9.4: VAS geïntegreerd in Ethernet-centralenetwerk

Om te voorkomen dat multicast-verkeer dat relevant is voor EN 54-2 wordt verzonden naar de router, gebruikt u de Ethernet-switch (over het algemeen MM, BPA-ESWEX-RSR20) die is goedgekeurd met centraleversie 2.8. Activeer IGMP-snooping van de Ethernet-switch, zie het desbetreffende gedeelte in het hoofdstuk Installatie van de Netwerkhandleiding.
Het branddetectiesysteem moet voorzien in de stroom voor de Ethernet-switch.

10 Installatie

Controlelijst

Lees alle punten hieronder goed door, voordat u begint met de installatie van het netwerk.

- Ethernet en CAN
  - De vereiste lijnlengte van de Ethernet TX-, Ethernet FX - en CAN TX- en CAN FX-kabels is korter dan de maximale lengte.
  - Alle randapparaten en hun bekabeling in de afzonderlijke centrales zijn gepland.
- Netwerkplanning
  - Alle IP-adressen en netwerkinstellingen voor de afzonderlijke centrales en extra netwerkonderdelen zijn gepland en beschikbaar.
  - Er is een overzicht beschikbaar van de extra onderdelen die moeten worden geïnstalleerd, zoals Ethernet-switches en media-omvormers en de bekabeling hiervan naar aangrenzende centrales.
  - Er is een overzicht beschikbaar van de netwerktopologie die moet worden geïnstalleerd.
  - Alle redundantie-instellingen voor het netwerk zijn gepland en beschikbaar.

10.1 Instellingen op media-omvormer

Er zijn slechts een paar stappen nodig om de media-omvormer te gebruiken:

– Stel de DIP-schakelaars in.
– Verbind de media-omvormer met de FX-netwerkkabels en de CAT5e-netwerkkabels.
– Geef de media-omvormer voeding via de interne BCM-accucontrollermodule.

Opmerking!
De media-omvormers krijgen alleen voeding via voedingsaansluiting 1.
De fout-LED op de media-omvormer brandt daarom continu. Dit heeft echter geen invloed op de functionaliteit van het apparaat.

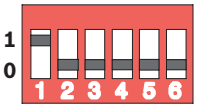
Opmerking!
Gebruik alleen een van de volgende kabels voor het netwerk:
Ethernet-kabel
Ethernet-patchkabel, afgeschermd, CAT5e of beter.
Let op de minimale buigradius in de kabelspecificatie.
Glasvezelkabel
Multimode: glasvezel Ethernet-patchkabel, duplex I-VH2G 50/125µ of duplex I-VH2G 62.5/125µ, SC-stekker.
Enkele modus: glasvezel Ethernet-patchkabel, duplex I-VH2E 9/125µ.
Let op de minimale buigradius in de kabelspecificatie.

Opmerking!
Raadpleeg de installatiehandleidingen van de montagesets voor informatie over het installeren van een media-omvormer in de behuizing van een paneel: FPM 5000 KMC(F.01U.266.845)FPM-5000-KES(F.01U.266.844)

Opmerking!
De maximale transmissiesectie voor media-omvormers in multimodus via FX is 2000 m.
De maximale transmissiesectie voor media-omvormers in singlemode via FX is 40 km.

Configureer de media-omvormer met de DIP-schakelaars zoals is weergegeven in de volgende afbeelding.

Opmerking!
Wijzig de DIP-switchinstellingen op media-omvormers alleen wanneer deze niet van energie worden voorzien.



DIP-schakelaarnummer	Instelling
1	Link-Fault-Pass-Through geactiveerd
2	Ethernet: automatische modus
3	Ethernet: 100 MBit
4	Ethernet: full-duplex
5	Glasvezelkabel: full-duplex
6	Link-down: uit

10.2 Ethernet-switch installeren

Waarschuwing!
Laserlicht
Kijk niet rechtstreeks in de straal met het blote oog of met visuele instrumenten (zoals een vergrootglas of microscoop). Als u dat toch doet, is dat gevaarlijk voor uw ogen op een afstand van minder dan 100 mm. Het licht komt tevoorschijn bij de visuele klemmen of aan het einde van de glasvezelkabels die hierop zijn aangesloten. Lichtgevende diode van klasse 2M, golflengte 650 nm, uitgang < 2 mW, voldoet aan IEC 60825-1.

Opmerking!
Raadpleeg: Installatiehandleiding voor de Montagekit voor Ethernet-switch FPM-5000-KES (F.01U.260.523).

10.3 Instellingen op switch

Om de switches te kunnen gebruiken in het netwerk, moet u ze programmeren.
Verbind uw laptop met het netwerk en gebruik de HiDiscovery-software die door de fabrikant is geleverd voor de initiële programmering van de switches. Zoek met deze software naar de switches in het netwerk. Dubbelklik op een switch om deze te selecteren en wijs er een IP-adres aan toe.
Na de initiële programmering van het IP-adres kunt u in een webbrowser de gebruikersinterface van de configuratie voor de switch ophalen.

Opmerking!
Raadpleeg de gebruikershandleiding van de fabrikant voor een exacte omschrijving van de installatie en de configuratie van de switches. Toegangsgegevens:
Gebruiker: admin
Wachtwoord: private

Open in een browser de gebruikersinterface voor de configuratie van de switches.
U moet de volgende taken uitvoeren in de switch:
- *IP-adres toewijzen, pagina 51*,
- *Redundantie-instellingen programmeren, pagina 52*.

Meer optionele instellingen, bijvoorbeeld:
- *Het storingsrelais programmeren, pagina 52*,
- *Verbindingsbewaking programmeren, pagina 53*,
- *IGMP-snooping activeren, pagina 54*.

10.3.1 IP-adres toewijzen

Opmerking!
Handige tip:
Gebruik in het apparaatgedeelte van IP-adressen voor switches nummers die hoger zijn dan 200 (xxx.xxx.xxx.200), als dit is toegestaan in uw netwerkconfiguratie. Zo is het adres duidelijker onderscheiden van de host-id van een IP-adres.
Voorbeeld:
Switch 192.168.1.201 is toegewezen aan de centrale met IP-adres 192.168.1.1.

Opmerking!
Raadpleeg de volgende documenten van de fabrikant voor een exacte beschrijving van de installatie en de configuratie van de switches:
Installatiehandleiding voor gebruikers
Naslaggids voor webinterface

Ga in een browser naar de gebruikersinterface van de configuratie voor de switch.
Stel in het menu **Basic Settings (Basisinstellingen) -> Network (Netwerk)** de volgende waarden in, afhankelijk van de gekozen topologie:
- Modus: lokaal
- IP-adres: het vereiste IP-adres, bijv. 192.168.1.201
- Netwerkmasker: het vereiste netwerkmasker, bijv. 255.255.255.0
- Gateway: de vereiste gateway, bijv. 192.168.1.254, of 0.0.0.0 als er geen gateway is vereist.

Klik op **Write** (Schrijven).

Opmerking!
De instellingen van de afzonderlijke menuopties in de configuratie van de switch worden van kracht nadat u op **Write** (Schrijven) hebt geklikt.
De instellingen worden alleen permanent opgeslagen (d.w.z. dat ze ook bewaard blijven nadat het apparaat opnieuw is opgestart) als u onder **Basic Settings -> Load/Save** (Basisinstellingen -> Laden/Opslaan) in het veld **Save** (Opslaan) de optie **On the device** (Op het apparaat) selecteert en op de knop **Save** (Opslaan) klikt.

10.3.2 Redundantie-instellingen programmeren

Omdat FPA-centralenetwerken RSTP gebruiken als redundantieprotocol, moet u het protocol activeren en programmeren in de gebruikersinterface van de configuratie:
Stel in het menu **Redundancy (Redundantie) -> Spanning Tree (Spanning Tree) -> Global (Algemeen)** de volgende waarde in:
- Functie: aan
- Protocolversie: RSTP
- Protocolconfiguratie: gebruik dezelfde instellingen als voor de paneelcontrollers.

Klik op **Write (Schrijven)**.

Opmerking!
De instellingen van de afzonderlijke menuopties in de configuratie van de switch worden van kracht nadat u op **Write (Schrijven)** hebt geklikt.
De instellingen worden alleen permanent opgeslagen (d.w.z. dat ze ook bewaard blijven nadat het apparaat opnieuw is opgestart) als u onder **Basic Settings (Basisinstellingen) -> Load/Save (Laden/Opslaan)** in het veld **Save (Opslaan)** de optie **On the device (Op het apparaat)** selecteert en op de knop **Save (Opslaan)** klikt.

10.3.3 Het storingsrelais programmeren

Opmerking!
Het storingsrelais hoeft alleen te worden geprogrammeerd voor toepassingen waarbij ten minste aan een van de volgende vereisten is voldaan:
Er is een verbinding tussen twee switches. Dit is bijvoorbeeld mogelijk bij een backbone met sublussen.
De voeding naar de switch is als redundant ontworpen.

Opmerking!
Raadpleeg de volgende documenten van de fabrikant voor een exacte beschrijving van de installatie en de configuratie van de switches:
Installatiehandleiding voor gebruikers
Naslaggids voor webinterface

Ga in een browser naar de gebruikersinterface van de configuratie voor de switch.
Stel onder **Diagnosis (Diagnose) -> Signal Contact (Signaalcontact)** op het tabblad **Signal Contact 1 (Signaalcontact 1)** de optie **Signal Contact Mode (Signaalcontactmodus)** in op **Device Status (Apparaatstatus)**.
Stel onder **Diagnosis (Diagnose) -> Device Status (Apparaatstatus)** in het veld **Monitoring (Bewaking)** de volgende waarden in:
– **Power Supply 1 (Voeding 1)**: **Monitor (Bewaken)**
– **Connection Error (Verbindingsfout)**: **Monitor (Bewaken)**
Alle andere instellingen moeten worden ingesteld op **Ignore (Negeren)**.

Opmerking!
De instellingen in **Device Status (Apparaatstatus)** gelden ook voor de storings-LED van de switch.

Klik op **Write (Schrijven)**.

Opmerking!
De instellingen van de afzonderlijke menuopties in de configuratie van de switch worden van kracht nadat u op **Write (Schrijven)** hebt geklikt.
De instellingen worden alleen permanent opgeslagen (d.w.z. dat ze ook bewaard blijven nadat het apparaat opnieuw is opgestart) als u onder **Basic Settings (Basisinstellingen) -> Load/ Save (Laden/Opslaan)** in het veld **Save (Opslaan)** de optie **On the device (Op het apparaat)** selecteert en op de knop **Save (Opslaan)** klikt.

10.3.4 Verbindingsbewaking programmeren

Opmerking!
U hebt de instelling voor verbindingsbewaking alleen nodig als u het storingsrelais van de switch gebruikt.

Als u het storingsrelais wilt gebruiken om de verbindingen van de switch te bewaken, moet u in de configuratie van de switch opgeven welke poorten van de switch moeten worden bewaakt.
Schakel het selectievakje **Forward Connection Errors (Verbindingsfouten doorsturen)** in voor de gewenste poorten in het menu **Basic Settings (Basisinstellingen) -> Port Configuration (Poortconfiguratie)**.
Alleen verbindingen waarvoor **Forward Connection Errors (Verbindingsfouten doorsturen)** is geactiveerd, worden bewaakt.
Klik op **Write (Schrijven)**.

Opmerking!
De instellingen van de afzonderlijke menuopties in de configuratie van de switch worden van kracht nadat u op **Write (Schrijven)** hebt geklikt.
De instellingen worden alleen permanent opgeslagen (d.w.z. dat ze ook bewaard blijven nadat het apparaat opnieuw is opgestart) als u onder **Basic Settings (Basisinstellingen) -> Load/ Save (Laden/Opslaan)** in het veld **Save (Opslaan)** de optie **On the device (Op het apparaat)** selecteert en op de knop **Save (Opslaan)** klikt.

10.3.5 QoS-prioriteit, alleen voor UGM-2040

Als u de switches gebruikt voor communicatie tussen brandmeldcentralenetwerken (BMC) en de UGM-2040, moet de QoS-prioriteit worden ingesteld in de switches van de UGM.
Wijzig in het menu QoS/Priorität -> Global de instellingen van het veld onder Trusted Mode in trustIpDscp.
Klik op **Write (Schrijven)**.

Opmerking!
De instellingen van de afzonderlijke menuopties in de configuratie van de switch worden van kracht nadat u op **Write (Schrijven)** hebt geklikt.
De instellingen worden alleen permanent opgeslagen (d.w.z. dat ze ook bewaard blijven nadat het apparaat opnieuw is opgestart) als u onder **Basic Settings -> Load/Save** (Basisinstellingen -> Laden/Opslaan) in het veld **Save** (Opslaan) de optie **On the device** (Op het apparaat) selecteert en op de knop **Save** (Opslaan) klikt.

10.3.6 IGMP-snooping activeren

Om te voorkomen dat EN 54-2-relevant multicast-verkeer wordt verzonden naar andere systemen die zijn aangesloten op de Ethernet Switch (gesproken woord ontruimingssysteem geïntegreerd in Ethernet-centralenetwerk, Remote Connect) activeert u IGMP-snooping.
Selecteer de volgende opties op de IGMP-configuratiepagina van de Ethernet Switch:

1. Schakel de bewerking **IGMP**-snooping in.
2. Activeer de **IGMP Querier (IGMP-querier)**.
3. Configureer het transmissie-interval waarmee de RSR20 IGMP-querypakketten verzendt (bijv. 4 seconden).
4. Configureer de tijd waarin multicast-groepsleden worden verondersteld te reageren op IGMP-query's (bijv. 3 seconden).
5. Selecteer **Discard (Negeren)** voor pakketten met onbekende multicast-adressen.
6. Selecteer **Send to Query and registered Ports (Verzenden naar query en geregistreerde poorten)** voor pakketten met bekende multicast-adressen.
7. Schakel IGMP alleen in voor poorten waarop andere systemen die zijn verbonden met de switch, zijn aangesloten. Schakel de optie **Static Query Port (Statische querypoort)** uit voor alle poorten.

10.4 CAN-netwerk

Netwerken en interfaces
De paneelcontroller heeft

- twee CAN-interfaces (CAN1/CAN2) voor netwerken (lus- of steeklijntopologie)
- twee signaalingangen (IN1/IN2)
- twee Ethernet-interfaces
- USB-interface

Afhankelijk van het type paneelcontroller:

- nog twee Ethernet-interfaces

– RS232-interface

De maximale kabellengte is 3 m voor een verbinding met de USB-interface en 2 m voor een verbinding met de RS232-interface.

Adressering en instellingen in het netwerk

Afhankelijk van het type paneelcontroller:

– Fysieke knooppuntadres ingesteld in de firmware van de centrale wanneer deze voor het eerst wordt ingeschakeld
– RSN op mechanische draaischakelaars aan de achterzijde van het paneel

Het fysieke knooppuntadres weergeven indien dit is opgeslagen in de paneelcontroller:

▸ Selecteer **Configuratie** -> **Netwerkservices** -> **Ethernet** -> **Ethernet-instellingen gebruiken** -> **IP-instellingen** -> **Stand.instellingen**

Het in de paneelcontroller opgeslagen fysieke knooppuntadres wijzigen:

▸ Geef de standaardinstellingen weer en wijzig het laatste nummer van **IP-adres**.

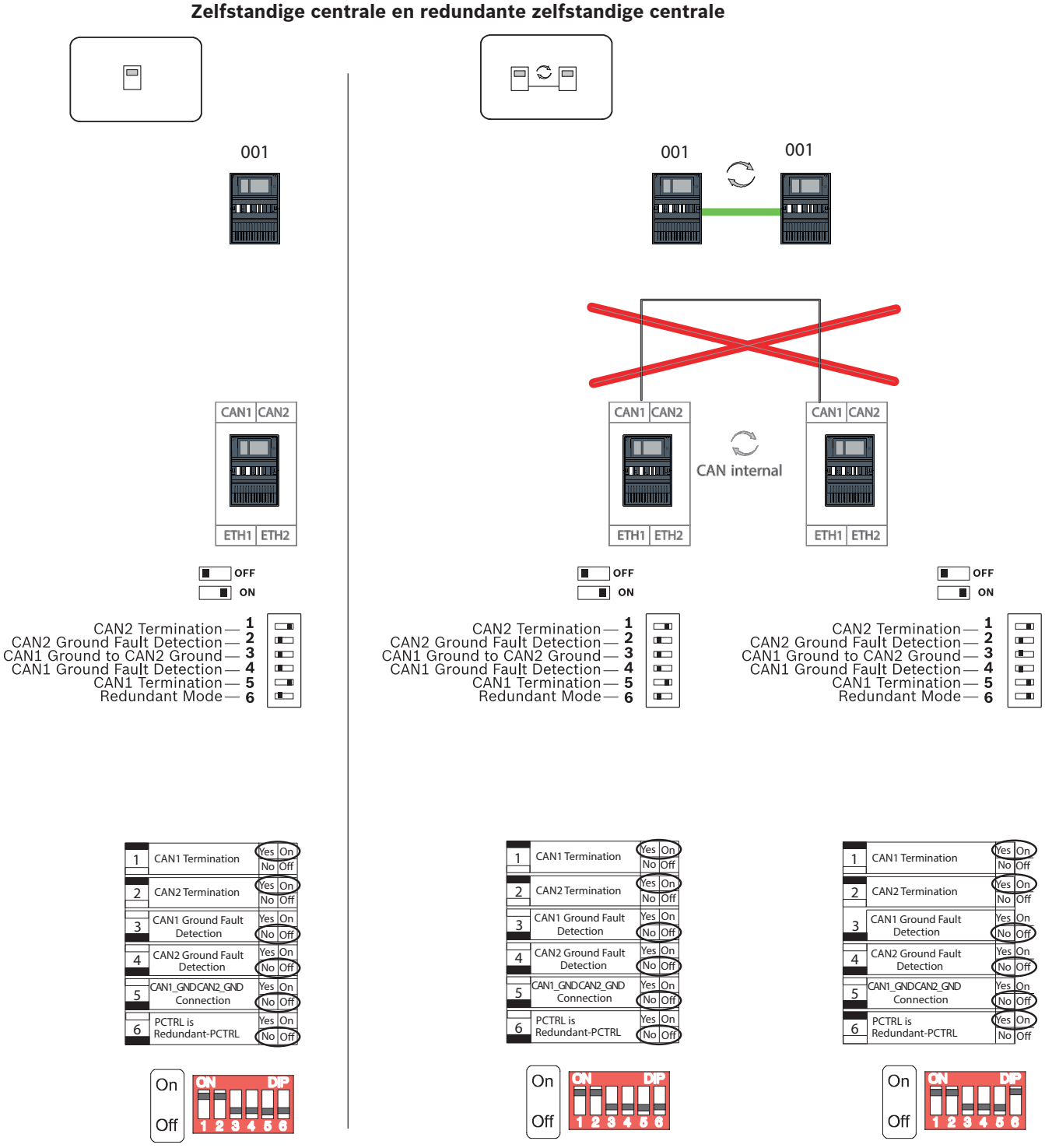
Een mechanisch RSN wijzigen:

▸ Bij mechanische draaischakelaars aan de achterzijde van de centrale stelt u het RSN in en noteert u dit op het label onder de draaischakelaars.

Configuratie van de topologie

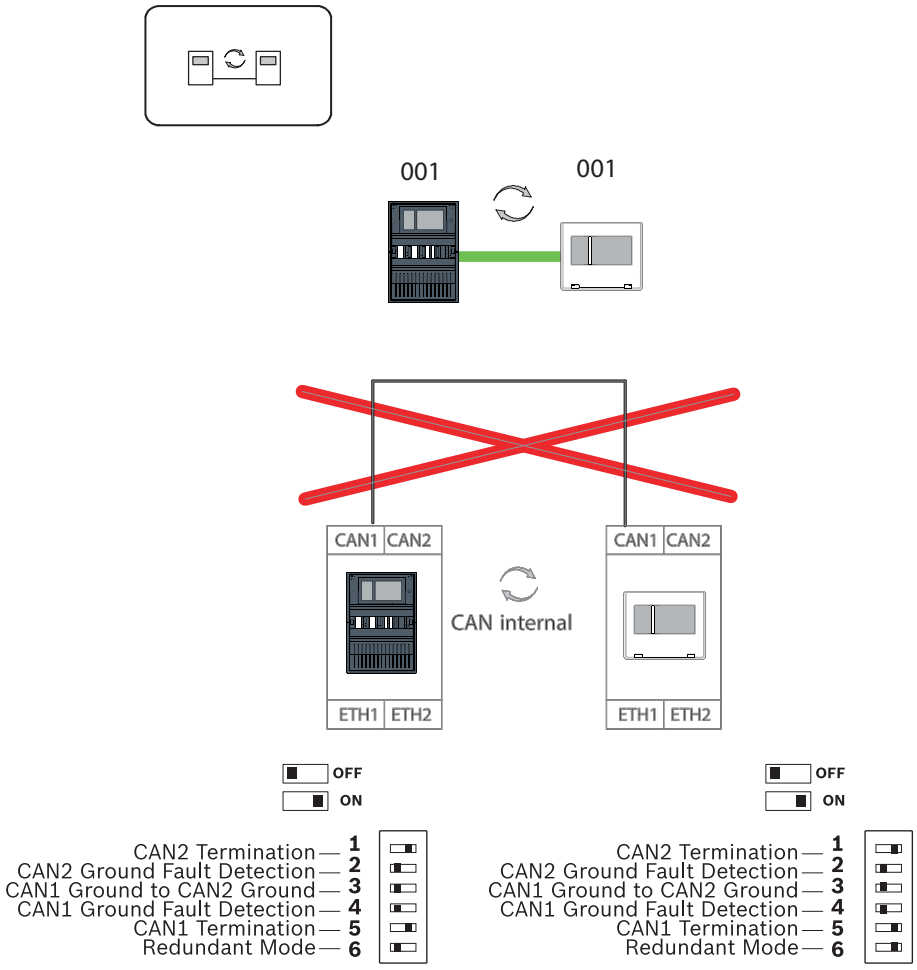
De DIP-switches voor de configuratie van verschillende topologieën bevinden zich aan de achterzijde.

▸ Markeer de geselecteerde instelling op het label bij de DIP-switches.

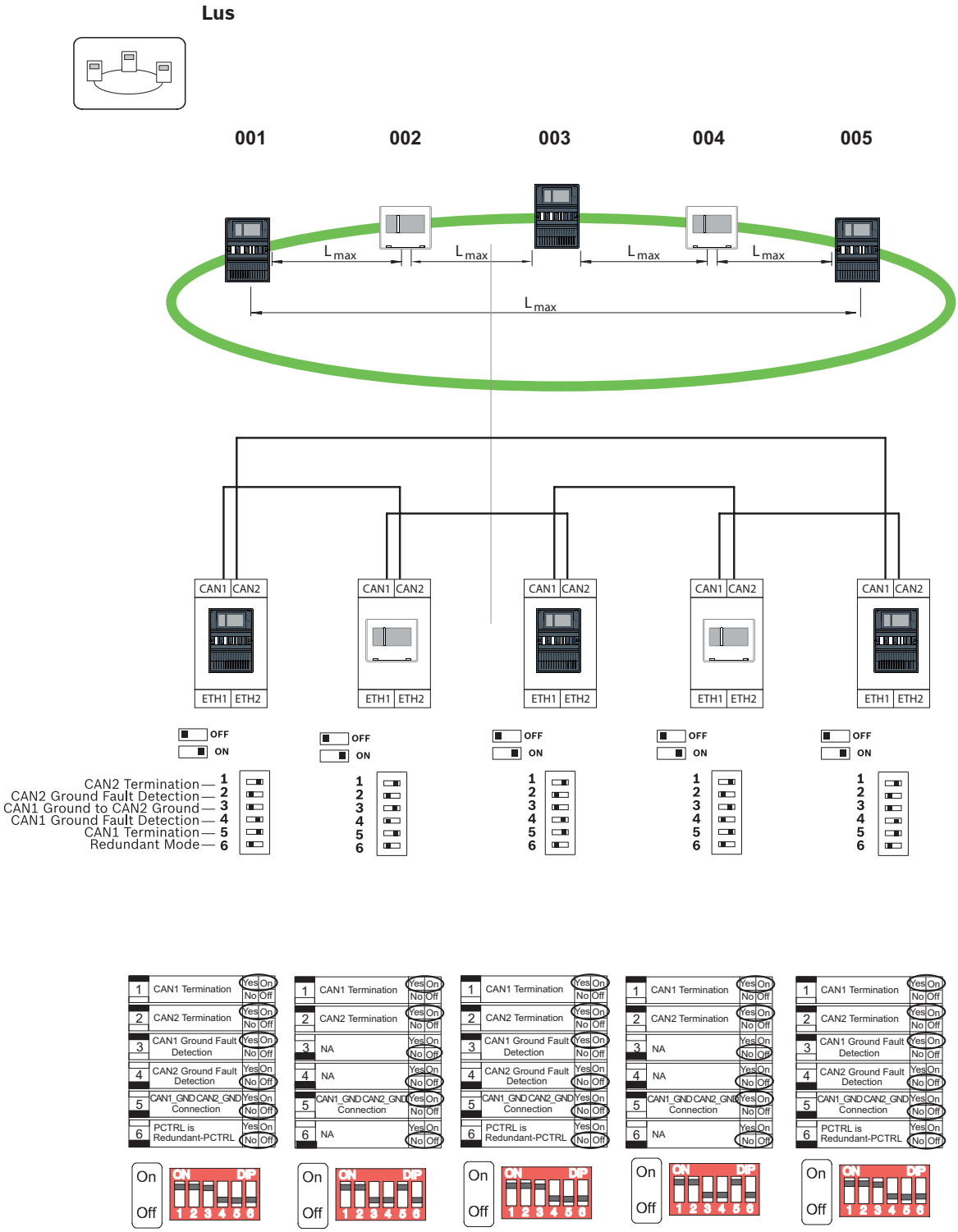


Afbeelding 10.1: Instellingen van DIP-switch voor zelfstandige centrale (boven: AVENAR, onder: FPA, links: normaal, rechts: redundant)

Extern bedieningspaneel als redundante paneelcontroller

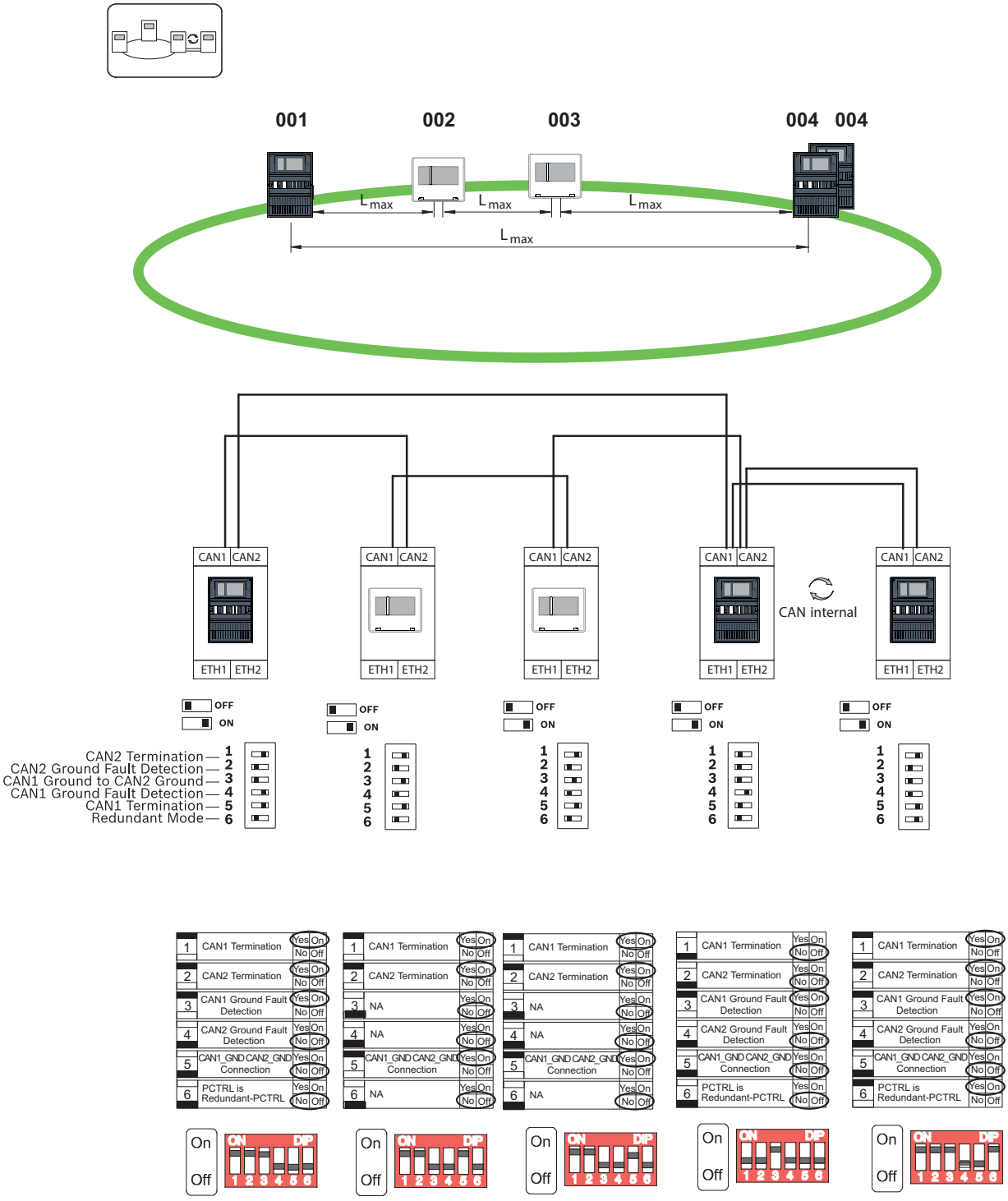


Afbeelding 10.2: Instellingen van DIP-switch voor extern bedieningspaneel als redundante centrale (alleen AVENAR)



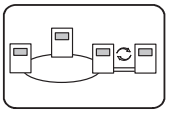
Afbeelding 10.3: Instellingen van DIP-switch voor lus (boven: AVENAR, onder: FPA)

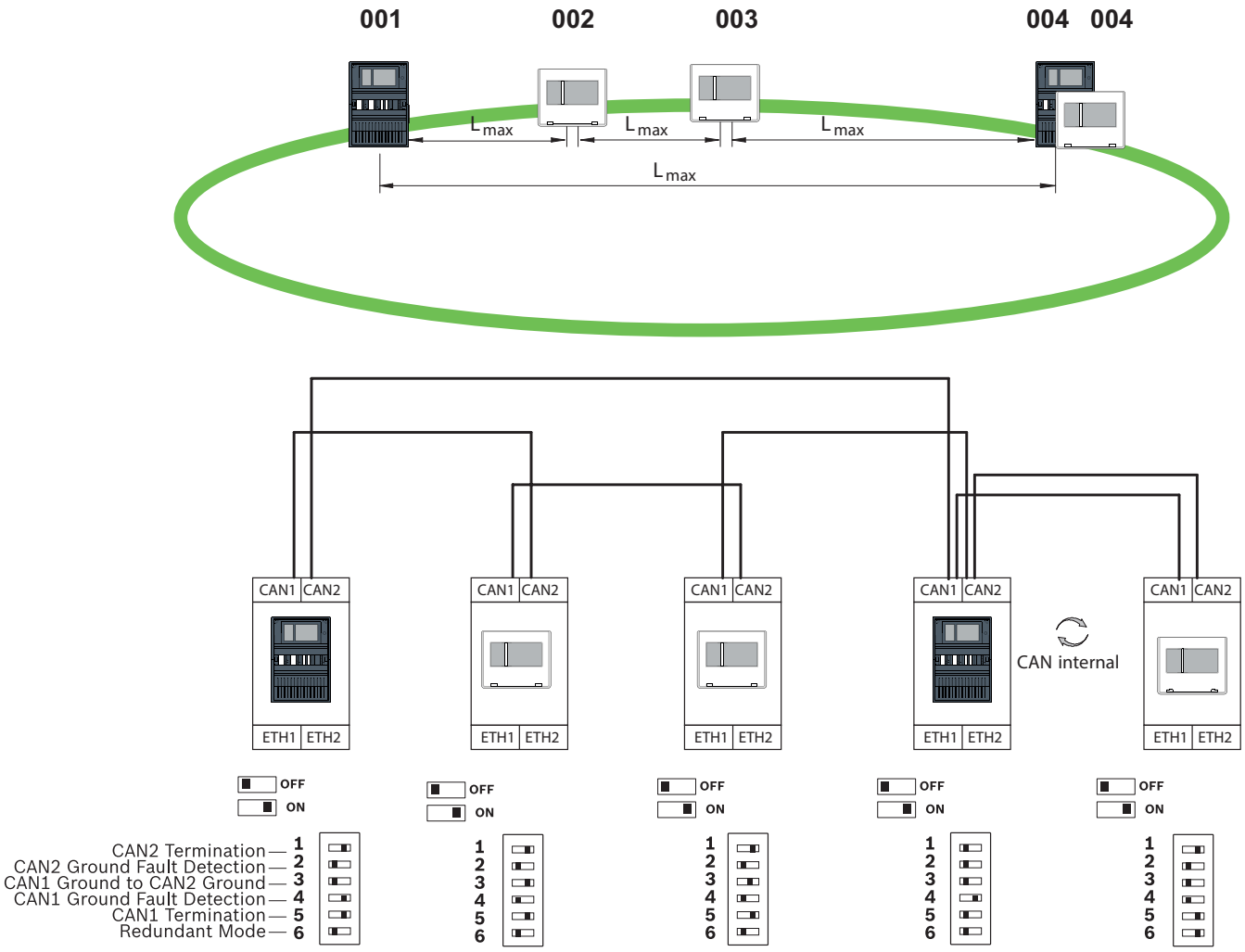
Lus met redundante centrales



Afbeelding 10.4: Instellingen van DIP-switch voor lus met redundante centrales (boven: AVENAR, onder: FPA)

Lus met extern bedieningspaneel als redundante centrale





Afbeelding 10.5: Instellingen van DIP-switch voor lus met extern bedieningspaneel (alleen AVENAR)

11 Bekabeling

Voor een systeem dat voldoet aan EN 54-2 moeten de RSTP-switches en de media-omvormers worden verbonden via de bewaakte voeding van de brandmeldcentrale.

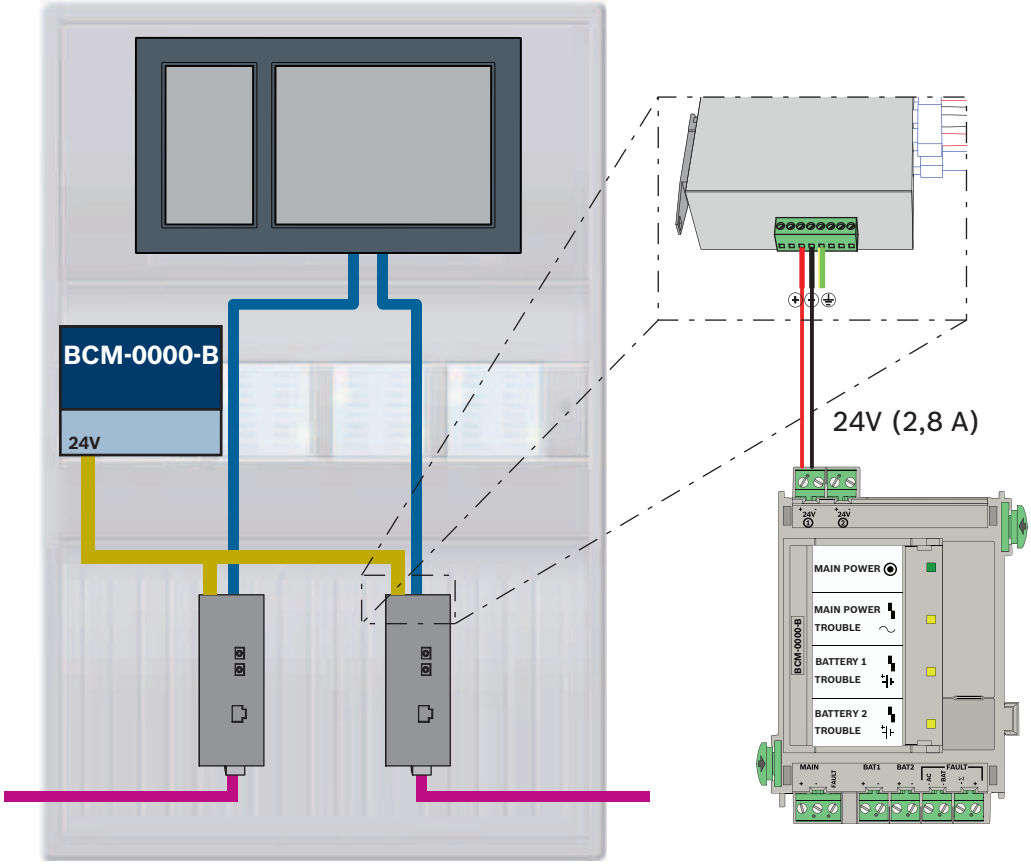
- Gebruik voor de voeding aan de media-omvormers en de RSTP-switches de 24 V-uitgang van de BCM 0000 B of de FPP-5000.
- Als u een redundante voeding hebt aangesloten of als u een verbinding van switch naar switch maakt, moeten de storingsuitgangen van de RSTP-switch worden bewaakt via centrale-ingangen. Gebruik bijvoorbeeld de ingangen op de paneelcontroller of IOP 0008 A.
- Bij gebruik van de media-omvormer moet de functie Link-Fault-Pass-Through worden geactiveerd. De configuratie wordt uitgevoerd via de DIP-switch van de media-omvormer.

Opmerking!
Gebruik alleen een van de volgende kabels voor het netwerk:
Ethernet-kabel
Ethernet-patchkabel, afgeschermd, CAT5e of beter.
Let op de minimale buigradius in de kabelspecificatie.
Glasvezelkabel
Multimode: glasvezel Ethernet-patchkabel, duplex I-VH2G 50/125µ of duplex I-VH2G 62.5/125µ, SC-stekker.
Enkele modus: glasvezel Ethernet-patchkabel, duplex I-VH2E 9/125µ, SC-stekker.
Let op de minimale buigradius in de kabelspecificatie.

11.1 Media-omvormer

Media-omvormers verbinden

Opmerking!
Let op de transmissierichting van de FOC-vezels wanneer u de FX-bekabeling van de media-omvormers aansluit.



Afbeelding 11.1: Verbinding van media-omvormer met de voeding en de paneelcontroller IN1/IN2

Pictogram	Omschrijving
	TX Ethernet-kabel (koper)
	FX Ethernet-kabel (glasvezelkabel)
	24 V voeding

Pictogram	Omschrijving
	Transmissie van storing
	Media-omvormer

11.2 Ethernet-switch

Switches aansluiten

U kunt de storingsuitgangen van de switches verbinden met de ingangen van de paneelcontroller of een IOP in- en uitgangsmodule.

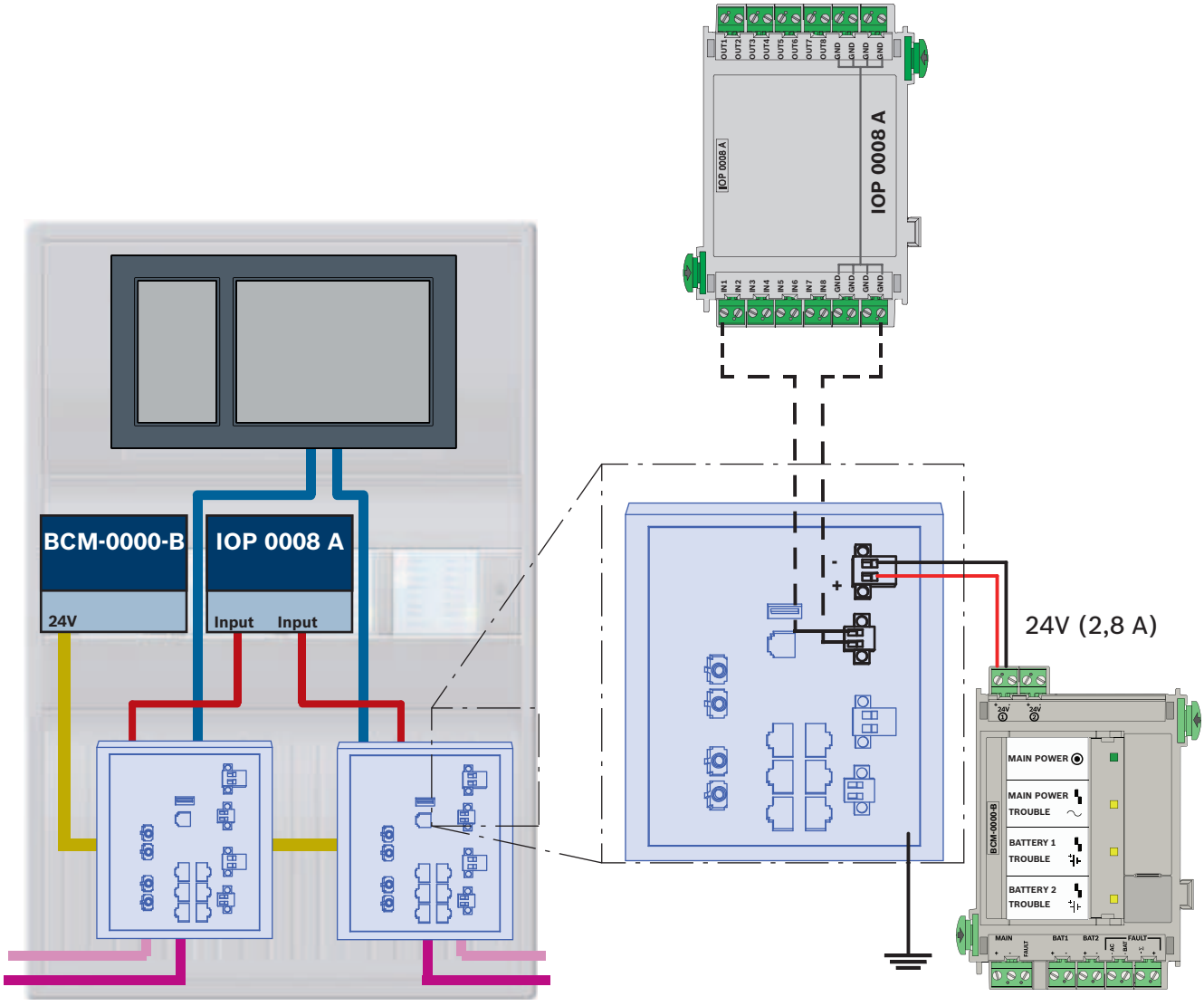
Opmerking!

Het storingsrelais moet alleen worden verbonden voor toepassingen waarbij ten minste aan een van de volgende vereisten is voldaan:

Er is een verbinding tussen 2 switches. Dit is bijvoorbeeld mogelijk bij een backbone met sublussen.

De voeding naar de switch is als redundant ontworpen.

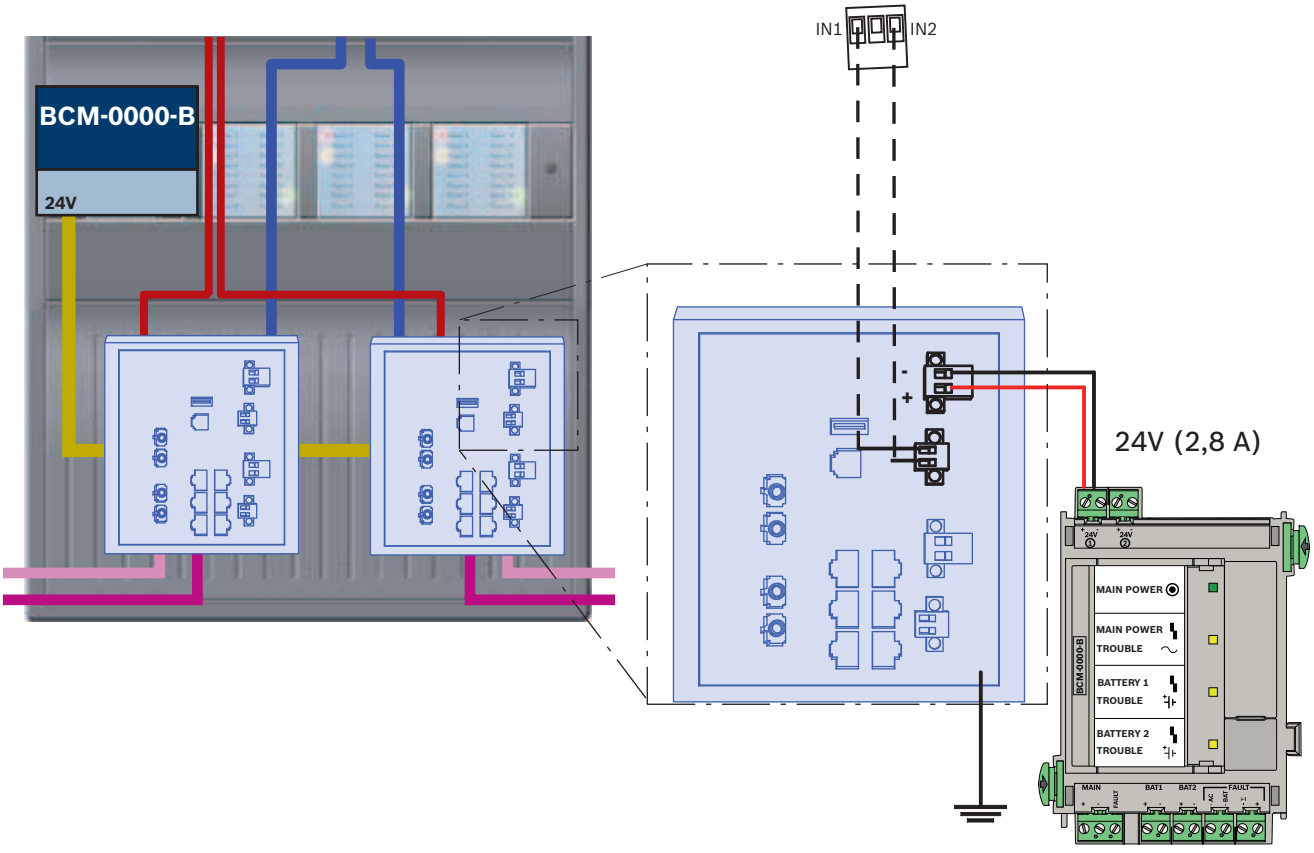
Verbinding van switches met storingsrapportage met de ingangen van de IOP-module:



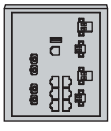
Afbeelding 11.2: Verbinding van switch met de voeding en IOP

Pictogram	Omschrijving
	TX Ethernet-kabel (koper)
	FX Ethernet-kabel (glasvezelkabel)
	24 V voeding
	Transmissie van storing
	RSTP-switch

Verbinding van switches met storingsrapportage met de ingangen van de paneelcontroller



Afbeelding 11.3: Verbinding van switch met de voeding en de paneelcontroller

Pictogram	Omschrijving
	TX Ethernet-kabel (koper)
	FX Ethernet-kabel (glasvezelkabel)
	24 V voeding
	Transmissie van storing
	RSTP-switch

Opmerking!
Gebruik de meegeleverde netwerkkabel niet om de switches te verbinden.
Gebruik een Ethernet-patchkabel, afgeschermd, CAT5e of beter.

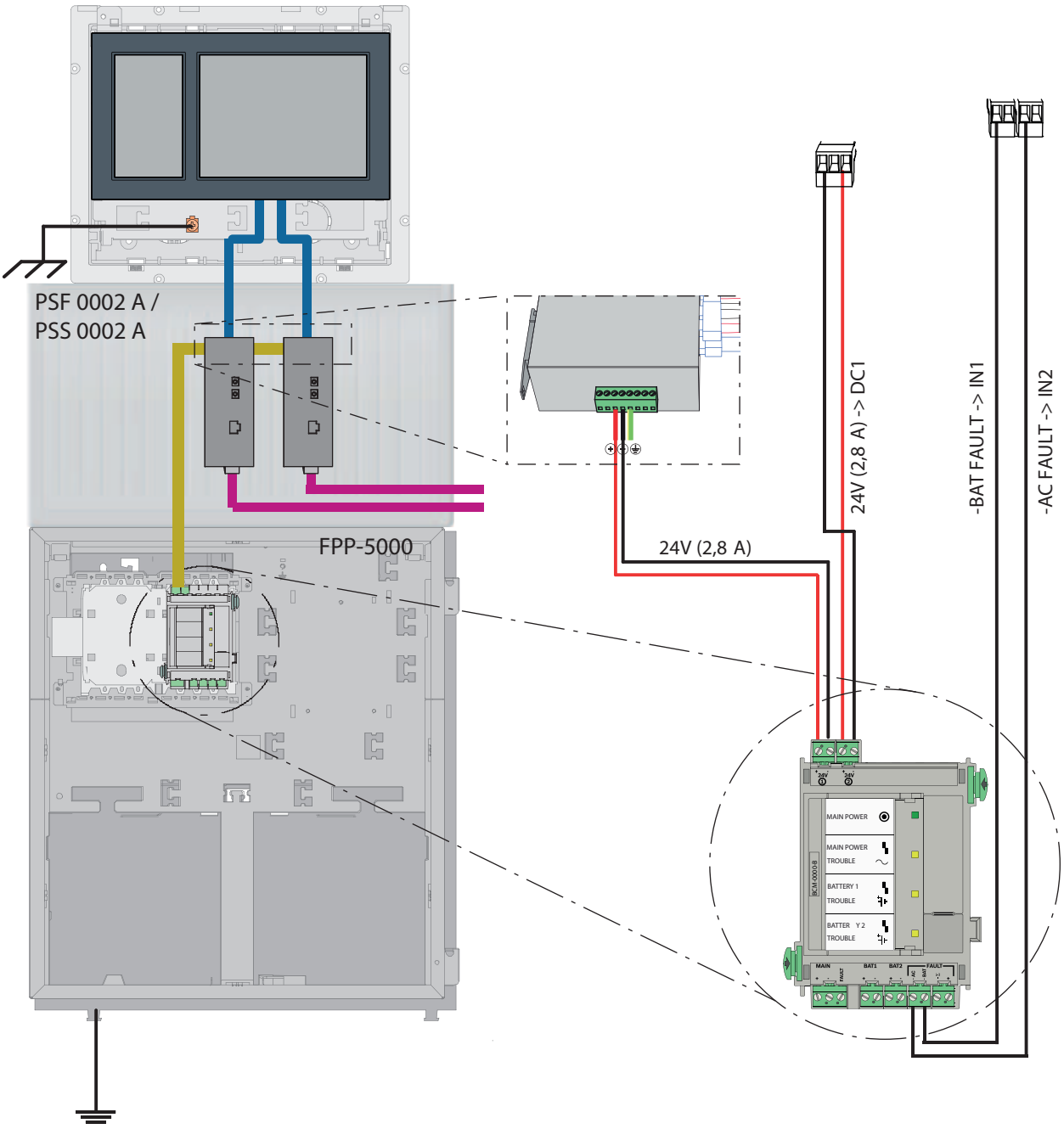
11.3 Extern bedieningspaneel

Een extern bedieningspaneel moet worden gevoed via een externe FPP-5000 voeding. De verbinding met het netwerk wordt tot stand gebracht via 2 media-omvormers in een PSS 0002 A of USF 0000 A.

Opmerking!
Houd er rekening mee dat de externe voeding FPP-5000 en de PSF 0002 A (PSS 0002 A) in de directe omgeving (zonder tussenruimte) van het externe bedieningspaneel moeten worden geïnstalleerd. De verbindingskabels tussen de componenten mogen niet kunnen worden aangeraakt, aangezien ze niet worden bewaakt op kortsluiting en onderbreking door lekstroom.

Opmerking!
Gebruik alleen media-omvormers om een extern bedieningspaneel te verbinden met een Ethernet-centralenetwerk.
Het gebruik van switches is niet toegestaan voor het externe bedieningspaneel.

Opmerking!
De functionele aarding van het externe bedieningspaneel moet altijd worden geplaatst wanneer het bedieningspaneel wordt verbonden met een Ethernet-centralenetwerk.



Afbeelding 11.4: Bekabeling van extern bedieningspaneel

Pictogram	Omschrijving
	TX Ethernet-kabel (koper)
	FX Ethernet-kabel (glasvezelkabel)
	24 V voeding
	Media-omvormer

12 Instellingen van FSP-5000-RPS

U kunt het gehele netwerk programmeren met de RPS-programmeersoftware via de USB-poort, de netwerkinterface of de seriële interface van een centrale. Hiervoor moet u de netwerkinstellingen hebben geconfigureerd op de centrale en de centrale opnieuw hebben opgestart om het netwerk in bedrijf te nemen.
In plaats hiervan kunt u ook de netwerkinterface gebruiken van een switch die is verbonden met het netwerk.

12.1 Netwerkknooppunten

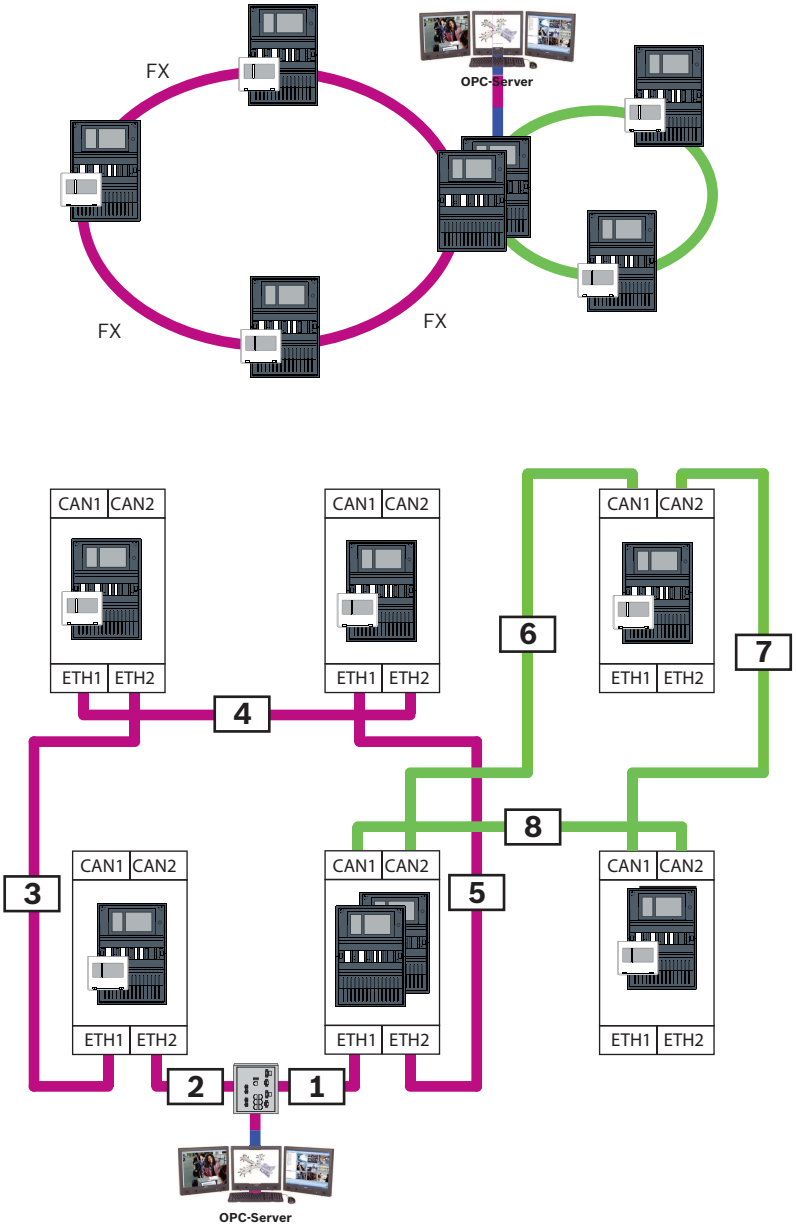
U moet het gehele netwerk met alle FPA-netwerkknooppunten programmeren in de FSP-5000-RPS-programmeersoftware en uploaden naar het netwerk. Ga hiervoor als volgt te werk:

- Verbind de FPA-knooppunten
  - Stel het RSN in op de afzonderlijke knooppunten
- Stel de lijnnummers van de netwerkbekabeling in volgens de geplande topologie
- Controleer of de topologieweergave correct is
- Verbind als het nodig is de OPC-server, het gesproken woord ontruimingssysteem, de UGM-2040-server en de switches
- Bewerk de Ethernet- en de IP-configuratie
  - Wijs de IP-adressen toe of gebruik de standaardinstellingen bij een topologie met minder dan 20 RSTP-switches
  - Kies het juiste redundantieprotocol voor de ingestelde topologie
- Voer een consistentiecontrole uit
- Verbind het netwerk via Ethernet, USB of de seriële interface
- Meld u meerdere keren aan
- Voer een volledige automatische detectie uit voor elke centrale
- Vraag de configuratiegegevens op en voltooi alle taken

Controleer of er foutmeldingen zijn na het opnieuw opstarten van het netwerk en corrigeer eventuele fouten.

12.2 Lijnnummers

U moet aan elke verbinding met het gebruikte netwerk een lijnnummer toewijzen. Het maakt niet uit of het een CAN-verbinding of een Ethernet-verbinding is.
U kunt hetzelfde lijnnummer gebruiken voor een CAN-verbinding en een Ethernet-verbinding. Voor een beter overzicht van de verbindingen moet u echter verschillende nummerbereiken gebruiken.
Houd er rekening mee dat als u **Netwerk** gebruikt als **Lijntype** in het venster **Net-interface**, het lijnnummer 0 moet zijn voor alle verbindingen.



Afbeelding 12.1: Voorbeeld van een netwerk en de mogelijke lijnnummering

12.3 Switches

Als u switches gebruikt in uw netwerk, moet u deze switches maken in de FSP-5000-RPS-programmeersoftware. U kunt maximaal 128 poorten toewijzen aan elke gemaakte switch. Om uw netwerk te maken, kunt u de verbonden lijnnummers toewijzen aan de afzonderlijke poorten.

12.4 OPC-servers

OPC-servers in uw netwerk moeten worden toegevoegd aan de programmeersoftware FSP-5000-RPS.

U moet de volgende instellingen gebruiken in de FSP-5000-RPS-software en op de OPC-server:

- Netwerkknooppunten
- Netwerkgroep
- RSN
- IP-adres

– Poort

De OPC-server maakt standaard gebruik van poort 25000.

Opmerking!

EN 54

De aansluiting van een gebouwbeheersysteem (bijv. BIS) via een Ethernet-interface met gebruikmaking van een OPC-server of een FSI-server is conform EN54 als de functies die relevant zijn voor EN54, alleen door de brandmeldcentrale worden uitgevoerd. Voor elke besturings- of beheerfunctie met EN54-relevantie (bijv. de besturing van signaleringsapparaten of het beheer van uitschakeling) door het gebouwbeheersysteem is een afzonderlijke EN54-certificering van het algehele systeem door een certificeringsinstantie vereist.

Opmerking!

De programmeersoftware FSP-5000-RPS

U moet een OPC-server toewijzen aan elk netwerkknooppunt waarvan de status moet worden verzonden.

12.5 UGM-2040-servers

Opmerking!

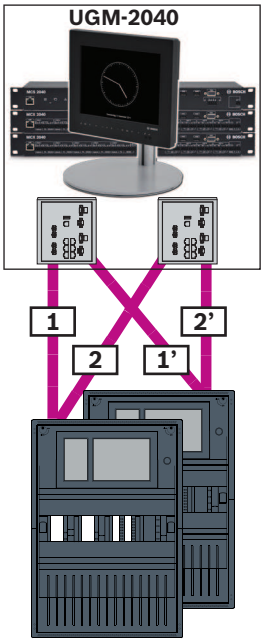
Alle paneelcontrollers en UGM-servers moeten zich in hetzelfde subnetwerk bevinden en hetzelfde multicast-adres hebben.

Als er meerdere centraleconfiguraties of netwerken zijn, moeten deze zich in hetzelfde subnetwerk bevinden. De multicast-adressen moeten verschillend zijn.

Opmerking!

U moet de UGM-2040-server toewijzen aan elk netwerkknooppunt waarvan de status moet worden verzonden.

Om een centrale met de UGM-2040 te verbinden, moet u de fysieke structuur van het netwerk simuleren in RPS. Hiertoe behoren ook de nummers van de lijnen tussen de verbonden paneelcontroller en de switches van de UGM-2040.



Afbeelding 12.2: Voorbeeld van lijnnummering voor de UGM-2040

13 Bijlage

13.1 Ethernet-foutmeldingen

Let erop dat in het geval van een fout de foutmelding plus de groepsfout worden weergegeven in elk exemplaar.

Fysiek adres	Logisch adres	Foutmelding	Omschrijving en mogelijke oorzaak
Groepsstoringen in verband met algemene netwerkstoringen			
135.0.1.0	Netwerk 1.0	**Algemene netwerkstoring**	Er is een incompatibele versie van de centralenetwerksoftware. Er zijn 2 verschillende softwareversies
Groepsstoringen in verband met het netwerk			
135.0.6.1	Netwerk 2.1	**Dubbel IP-adres**	Een IP-adres is twee keer toegewezen.
135.0.6.2	Netwerk 2.2	**IP-instellingen**	De IP-configuratie van de rapportagecentrale is anders dan de RPS-configuratie
135.0.6.3	Netwerk 2.3	**Redundantie-instellingen**	De redundantieconfiguratie (RSTP, RSTP-parameter, dual homing of niets) van de rapportagecentrale is anders dan de RPS-configuratie.
Groepsstoringen in verband met RSTP (Rapid Spanning Tree Protocol)			
135.0.7.1	Netwerk 3.1	**RSTP Fallback**	De rapportagecentrale is overgeschakeld van RSTP-modus naar STP-modus (compatibiliteitsmodus). Er is een STP-apparaat verbonden met het netwerk.
135.0.7.2	Netwerk 3.2	**Wijziging RSTP-topologie**	De RSTP-netwerktopologie is gewijzigd. Er is bijvoorbeeld een ander RSTP-apparaat toegevoegd aan het netwerk. Deze melding kan ook worden weergegeven bij een onderbreking in de lijn.

Fysiek adres	Logisch adres	Foutmelding	Omschrijving en mogelijke oorzaak
135.0.7.3	Netwerk 3.3	**RSTP-koppelingstype Point2Point**	Een RSTP-poort van de rapportagecentrale heeft niet de status point-to-point. Er zijn bijvoorbeeld meerdere RSTP-apparaten verbonden met een RSTP-poort. Of een ander RSTP-apparaat is met de RSTP-poort verbonden via een half-duplex lijn.
Groepsstoringen in verband met netwerkverbindingen			
135.0.5.1	Netwerkverbinding 1.0	**Storing CAN 1**	Gegevenstransmissie naar CAN-bus 1 is beperkt. Mogelijke oorzaken: kabelbreuk, kabel niet verbonden, kabelinterferentie.
135.0.5.2	Netwerkverbinding 2.0	**Storing CAN 2**	Gegevenstransmissie naar CAN-bus 2 is beperkt. Mogelijke oorzaken: kabelbreuk, kabel niet verbonden, kabelinterferentie.
135.0.5.3	Netwerkverbinding 3.0	**Storing Ethernet 1**	Gegevenstransmissie naar Ethernet-lijn 1 is beperkt. Mogelijke oorzaken: kabelbreuk, kabel niet verbonden, kabelinterferentie.
135.0.5.4	Netwerkverbinding 4.0	**Storing Ethernet 2**	Gegevenstransmissie naar Ethernet-lijn 2 is beperkt. Mogelijke oorzaken: kabelbreuk, kabel niet verbonden, kabelinterferentie.

Index

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

Building solutions for a better life.

202202161634