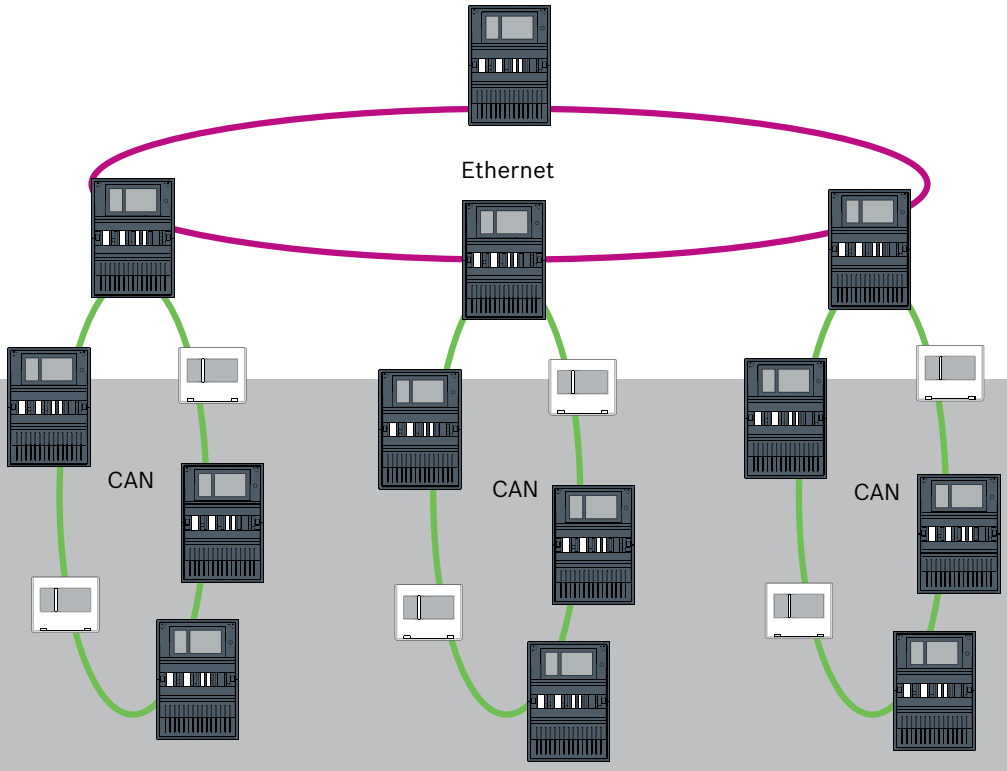
AVENAR panel | FPA-5000 | FPA-1200



ru Networking manual

Содержание

1 Безопасность

В этой главе описаны организационные меры для ПК, на которых выполняются клиенты служб для портфеля противопожарных продуктов Bosch. Вы обязаны соблюдать эти договорные соглашения.
Кроме того, здесь вы найдете примечания по безопасности, сортированные по разделам. В остальных разделах руководства примечания по безопасности размещаются перед соответствующей инструкцией.

1.1 Организационные меры для ПК, на которых выполняются клиенты служб

Введение

Портфель противопожарных продуктов Bosch включает программы для ПК (клиенты служб), выполняемые на компьютере, который должен иметь установленное физическое подключение к системе пожарной сигнализации. В целях безопасности и соблюдения требований нормативных стандартов устанавливать систему пожарной сигнализации в общей сети запрещено. Это, в свою очередь означает, что для сетевой системы пожарной сигнализации и ПК, на котором выполняется клиент службы, необходимо создать выделенную физическую сеть. Поскольку Bosch разрабатывает только клиенты служб, но не производит ПК, на которых они выполняются, компания Bosch не может контролировать соответствующие компьютеры. В этом документе описан ряд организационных мер, которые позволят снизить связанные с этим риски безопасности.

Меры

Если описанные ниже процедуры требуют подключения к Интернету (либо клиент службы требует временного подключения к Интернету для лицензирования), ПК необходимо физически изолировать от сетевой системы пожарной сигнализации, прежде чем подключать ПК к Интернету. Интернет-подключение должно быть разорвано, прежде чем ПК снова будет подключен к сетевой системе пожарной сигнализации.

1. Операционные системы
   Bosch описывает предварительные требования для работы клиентов служб, включая версии операционной системы. Совместимость клиентов с этими версиями гарантируется. Необходимо регулярно обновлять операционную систему, в которой выполняется клиент, с целью устранения потенциальных уязвимостей безопасности. Необходимо настроить систему так, чтобы доступ с возможностью записи был открыт только к тем папкам, которые необходимы для выполнения соответствующей задачи. По умолчанию всем пользователям предоставляются разрешения только на чтение.
2. Антивирусное ПО
   Необходимо установить и запустить на компьютере современное антивирусное программное обеспечение. Необходимо регулярно обновлять файлы определений этого ПО.
3. Брандмауэр
   Необходимо установить и запустить на ПК программный брандмауэр. Его необходимо настроить так, чтобы обеспечить возможность трафика между клиентом службы и системой пожарной сигнализации, обновления операционной системы и работу антивирусного программного обеспечения. Весь остальной трафик должен блокироваться.

4. Безопасный вход пользователей
   Доступ к ПК должен ограничиваться операторами, использующими установленный клиент службы. Безопасность входа в систему необходимо гарантировать современными средствами защиты. Если для защиты доступа используется пароль, необходимо внедрить и выполнять современную политику паролей.
   Для повышения эффективности аутентификации рекомендуется соблюдать правило «двух человек» («принцип четырех глаз») или использовать многофакторную аутентификацию.
5. Программное обеспечение и службы
   Необходимо свести к минимуму объем программного обеспечения, устанавливаемого на ПК. Следует устанавливать только программное обеспечение, необходимое для работы клиента службы и выполнения соответствующих задач.
6. Ограничения на использование
   С помощью организационных мер необходимо ограничить использование ПК задачами, связанными с работой службы. Это, помимо прочего, подразумевает использование Интернета на этом ПК только в целях, описанных в этом документе.
7. Разделение обязанностей
   Необходимо разделить обязанности и зоны ответственности, чтобы снизить риск несанкционированного или случайного изменения или злоупотребления, то есть разные задачи следует назначать разным ролям.
8. Мониторинг
   Все попытки доступа к ПК, на котором выполняется клиент службы, необходимо отслеживать с целью своевременного распознавания несанкционированного доступа к ПК и Интернету.

1.2 Пояснение символов безопасности

Предупреждение!
Указывает на опасную ситуацию, которую если не избежать, ведет к серьезным травмам или смертельному исходу.

Внимание!
Предупреждение указывает на риск повреждения объектов.

Замечание!
Указывает на ситуацию, которая может привести к повреждению оборудования или окружающей среды либо потере данных, если не будут приняты меры.

1.3 Примечания по безопасности

Медиаконвертер

Предупреждение!
Лазерный источник света
Не смотрите на источник луча невооруженным глазом или через любые оптические приборы (например, увеличительное стекло, микроскоп). При несоблюдении этого требования возможна потеря зрения при дистанции менее 100 мм. Лазерный свет исходит из видимых контактов или на концах подключенных к ним оптоволоконных кабелей. Используется лазерный диод класса 2M, длина волны 650 нм, выходная мощность < 2 МВт, соответствует IEC 60825-1.

Remote Services

Внимание!
Для доступа через Интернет используйте только Remote Services компании Bosch.

Внимание!
Remote Services требуют безопасного IP-подключения. Требуется Bosch Remote Services или подключение к Private Secure Network.
Вместе с сетью Private Secure Network предоставляется IP-сеть на основе подключения DSL с дополнительным беспроводным доступом со стороны панели (EffiLink). Remote Services для Private Secure Network предоставляются только в Германии по соглашению об обслуживании с Bosch BT-IE.

Внимание!
Для построения централизованной сети пожарной сигнализации необходима выделенная сеть Ethernet.
Использование системы автоматического пожаротушения в любой другой сети Ethernet возможно исключительно на собственный ринк пользователя. Bosch не несет никакой ответственности и не предоставляет никаких гарантий в случае такого использования системы.
При отсутствии выделенной сети Ethernet надежность передачи тревожного сигнала и безопасность системы не гарантируются.

Интеллектуальная передача информации

Предупреждение!
Угрозы безопасности в сети Ethernet
Не подключайте PRAESENSA к FPA-5000/FPA-1200 с помощью Smart Safety Link из-за угрозы безопасности в сети Ethernet.

Замечание!
VdS 2540
Система речевого и аварийного оповещения должна быть установлена вплотную к пожарной панели в одном помещении. Иначе требования VdS 2540 для путей передачи данных не будут удовлетворены.

Сеть панелей

Замечание!
EN 54
В соответствии со стандартом EN 54 применяются только компоненты, сертифицированные для использования в сетях систем пожарной сигнализации. Внешние RSTP-коммутаторы и медиаконвертеры в сетях Ethernet должны быть установлены в корпусах панелей. Установка за пределами корпуса панели нарушает требования EN 54.

Замечание!
Длина кабеля TX
Все IP-подключения должны осуществляться напрямую или через медиаконвертеры, утвержденные Bosch. Длина кабеля TX между узлами должна быть менее 100 м.

Замечание!
VdS 2540 - Сеть Ethernet
Применительно к Ethernet-сетей панелей следует учитывать, что для установки в Германии, где требуется соответствие стандарту VdS 2540, для всех путей передачи данных должен использоваться оптоволоконный кабель. Единственным исключением является корпус.

Замечание!
Для стандартных приложений используйте стандартные сетевые параметры. Стандартные сетевые параметры разрешается изменять только опытным пользователям с соответствующими знаниями по организации сетей.

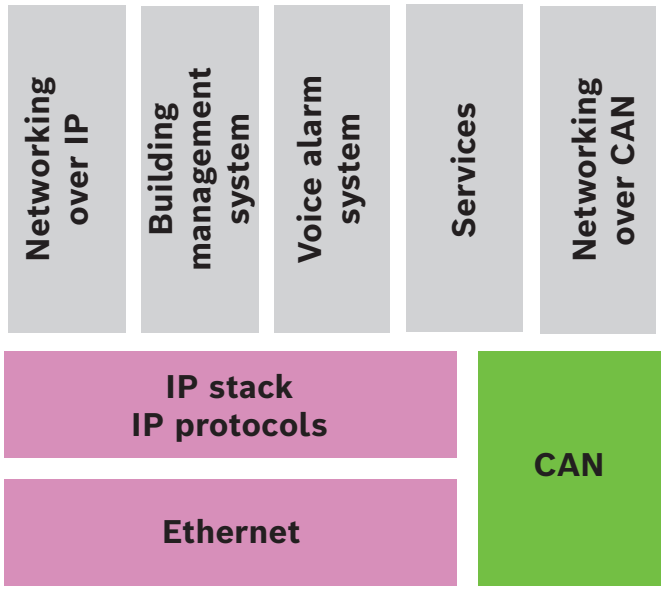
Замечание!
Применимые топологии
Функциональные возможности и связь между панелями зависят от типа панели. Для получения информации о службах, количестве подключаемых панелей, а также удаленных клавиатур см. спецификацию панели.

2 Введение

Этот документ предназначен для пользователей с опытом проектирования и установки систем пожарной сигнализации, соответствующих стандарту EN 54, а также с дополнительными знаниями по организации сетей. Кроме того, необходимо понимание принципов сетевого подключения.
В этом документе описываются различные сетевые топологии систем пожарной сигнализации. Топологии описываются независимо от типа пожарных панелей.
Для создания сетей панелей, соответствующих представленным топологиям, и подключения служб необходимо воспользоваться описанным в этом документе сетевым шаблоном.
В документе приводится обзор базовых условий, предельных значений и общих процедур планирования и установки сети панелей.
Монтаж отдельных компонентов подробно описывается в соответствующих руководствах по установке.
Описание пользовательского интерфейса контроллера панели см. в руководстве пользователя, прилагаемом к устройству.

Пользовательский интерфейс программного обеспечения для программирования FSP-5000-RPS описывается в интерактивной справке.

3 Обзор системы



В сети разные службы используют интерфейс Ethernet и протоколы IP. Интерфейс Ethernet можно отключить полностью или только для подключения через TCP/IP. Отключение данного интерфейса может потребоваться для сетевого подключения через CAN.

Включение служб

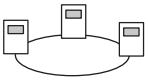
- Сетевое подключение через TCP/IP
  В FSP-5000-RPS в настройках сети Ethernet разрешите связь между панелями.
- система управления зданием
  Создать сервер в конфигурации FSP-5000-RPS
- Подключение системы речевого оповещения
  Добавьте систему речевого и аварийного оповещения в конфигурацию FSP-5000-RPS и настройте виртуальные триггеры.
- Remote Services (Remote Connect в качестве предварительного требования Remote Maintenance и Remote Alert)
  Установите в FSP-5000-RPS соответствующий флажок.
- Remote Services (Remote Connect в качестве предварительного требования, Remote Maintenance и Remote Alert) для Private Secure Network
  Добавьте удаленный доступ в конфигурацию FSP-5000-RPS и настройте удаленный доступ в FSP-5000-RPS.

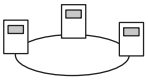
Замечание!
Непреднамеренная передача данных
Если интерфейс Ethernet контроллера панели используется только для связи с системой управления зданием или для Remote Services, отключите связь по TCP/IP между панелями в FSP-5000-RPS. В противном случае возможна непреднамеренная передача данных о пожаре через Ethernet.

Для работы со службами на основе Ethernet или TCP/IP необходимо включить интерфейсы Ethernet и задать правильные параметры TCP/IP.

Сеть панелей и удаленных клавиатур

В таблице показаны варианты сетевого подключения панелей/удаленных клавиатур в зависимости от топологии сети и типа панелей. Обратите внимание на ограничения, определяемые топологией сети.

Топология	**AVENAR panel 8000, премиум-лицензия**	**AVENAR panel 8000, стандартная лицензия.**	**AVENAR panel 2000, премиум-лицензия**	**AVENAR panel 2000, стандартная лицензия.**
 Автономная	Возможно	Возможно	Возможно	Возможно
 Кольцо	Не более 32 панелей/ удаленных клавиатур, возможность подключения панели AVENAR panel 2000 с расширенной лицензией и панели FPA	Не более 32 панелей/ удаленных клавиатур, возможность подключения панели AVENAR panel 2000 с расширенной лицензией и панели FPA	Не более 32 панелей/ удаленных клавиатуры, возможность подключения панели AVENAR panel 8000 и панели FPA	1 панель и не более 3 удаленных клавиатур
 Резервирование панелей	Резервный контроллер панели также должен иметь премиум-лицензию. В качестве резервного контроллера панели также можно использовать удаленную клавиатуру.	Резервный контроллер панели может иметь стандартную лицензию. В качестве резервного контроллера панели также можно использовать удаленную клавиатуру.	Невозможно	Невозможно

Топология	**FPA-5000**	**FPA-1200**
 Автономная	Возможно	Возможно
 Кольцо	Не более 32 панелей и удаленных клавиатур	1 панель и не более 3 удаленных клавиатур
 Резервирование панелей	Возможно	Невозможно (DIP 6 на контроллере панели не функционирует.)

При расширении сети FPA-5000 Bosch рекомендует делать это с помощью панели серии AVENAR panel.
При замене панели серии FPA на панель серии AVENAR panel достаточно заменить только контроллер панели. Помните, что панели серии AVENAR panel не поддерживают адресные карты. Если подключен коммутатор Ethernet, можно продолжить его использование.
При замене удаленной клавиатуры серии FPA на удаленную клавиатуру серии AVENAR panel убедитесь, что сопротивление линии соответствует диапазону, предусмотренному для удаленной клавиатуры серии AVENAR panel.

Замечание!
Установка микропрограмм
на всех подключенных панелях должны быть установлены микропрограммы одной и той же версии.
Установка микропрограммы возможна только для активной панели. Что касается резервных панелей, необходимо выполнить установку микропрограммы для обеих панелей. Для этого необходимо поменять роли панелей, а затем, после успешной установки микропрограммы, поменять роли еще раз.

Замечание!
Версии микропрограммы
Для системы, содержащей исключительно узлы AVENAR, рекомендуется использовать последнюю версию микропрограммы панели 4.x.
Для системы, содержащей хотя бы один узел FPA/FMR, рекомендуется использовать последнюю версию микропрограммы панели 3.x.

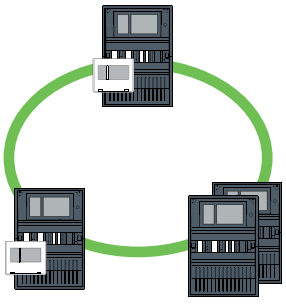
Замечание!
С 1 января 2022 г. до 31 декабря 2025 г. микропрограмма панелей версии 3.x находится в режиме обслуживания. В течение этого периода будут выпускаться новые версии, содержащие исправления критических ошибок и критических нарушений безопасности. Добавление новые функций продуктов, периферийных устройств LSN и языков графического интерфейса пользователя, а также внесение нормативных изменений не планируется.
После 31 декабря 2025 г. использование микропрограммы версии V3.x на панелях, подключенных к интерфейсу Ethernet или сети, повышает угрозу безопасности. Настоятельно рекомендуется выполнить оценку рисков безопасности. При обнаружении угрозы безопасности необходимо обновить панель до AVENAR panel и запустить новейшую микропрограмму версии V4.x.

Замечание!
Резервный контроллер панели
Невозможно объединить контроллер панели серии AVENAR panel с контроллером панели серии FPA для резервирования.

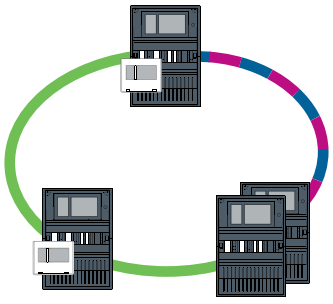
4 Топологии

В этом документе описываются различные сетевые топологии систем пожарной сигнализации. Топологии описываются независимо от типа пожарных панелей.

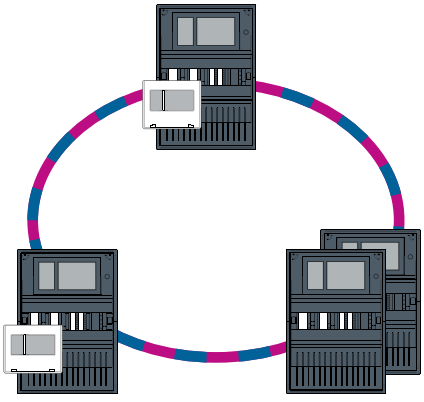
Замечание!
Применимые топологии
Функциональные возможности и связь между панелями зависят от типа панели. Для получения информации о службах, количестве подключаемых панелей, а также удаленных клавиатур см. спецификацию панели.



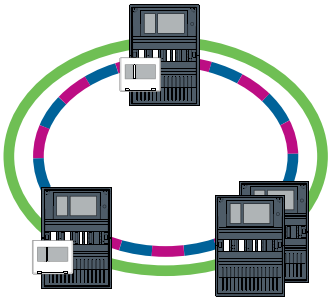
Кольцо CAN, Страница 16



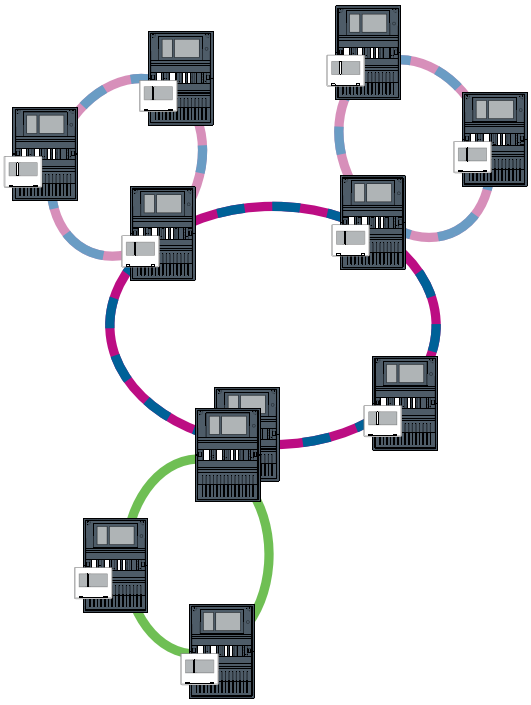
Кольцо CAN с сегментами Ethernet, Страница 17



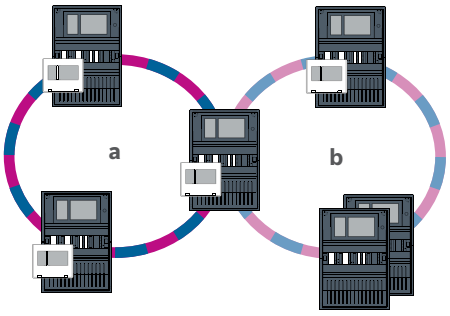
Кольцо Ethernet, Страница 17



Двойное кольцо Ethernet/CAN, Страница 17

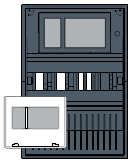
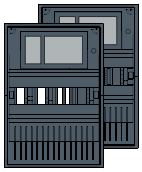
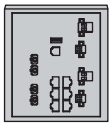


Магистраль Ethernet с кольцевыми подсетями (Ethernet/CAN), Страница 17



Подключение колец Ethernet, Страница 19

Кабель	Описание
	Кабель Ethernet TX (медный), длина кабеля TX между узлами < 100 м
	Кабель Ethernet FX (оптоволоконный)
	Кабель Ethernet TX или FX, длина кабеля TX между узлами < 100 м
	Кабель CAN, длина кабеля CAN между узлами < 1000 м

Устройство	Описание
	Панель или удаленная клавиатура (в топологии Ethernet по одному внутреннему RSTP-коммутатору на каждую)
	Панель или резервная панель (в топологии Ethernet — внутренний RSTP-коммутатор) Удаленную клавиатуру можно использовать в качестве резервного контроллера панели. Сетевые подключения и настройки для резервного контроллера панели и резервной клавиатуры идентичны. Использование резервной клавиатуры применимо только к AVENAR panel 8000.
	Коммутатор Ethernet в качестве внешнего RSTP-коммутатора (или универсальный коммутатор Ethernet MM)

Устройство	Описание
	Медиаконвертер
	Защищенный сетевой шлюз для Remote Services
	система управления зданием

Ограничения в сети

Сеть содержит узлы.

- Узел представляет собой контроллер панели, удаленную клавиатуру или сервер (BACnet, FSI-сервер, OPC-сервер или UGM-сервер).
- Максимальное количество узлов: 32.
- Максимальное количество логических точек в сети: 32768.
- Максимальное количество логических точек для каждой подключенной к сети панели: 2048.
- Максимальное количество удаленных клавиатур, которое можно назначить одной панели: 3.
- Максимальное количество серверов, которое можно назначить одной панели или удаленной клавиатуре:
  - 1 BACnet server
  - 2 FSI server
  - 1 OPC server
  - 2 UGM server

Дополнительную информацию см. в главе «Системные ограничения» в руководстве по системе.

В зависимости от предполагаемого применения различные контроллеры панели и удаленные клавиатуры можно разделить на группы и определить как сетевые или локальные узлы. Как правило, в любой заданной группе могут отображаться только состояния панелей этой группы. Состояния всех панелей могут отображаться и/или обрабатываться с сетевых узлов, независимо от группы, к которой принадлежат панели.

Адрес физического узла

Панель, удаленная клавиатура или сервер идентифицируется в сети с помощью уникального адреса, известного как адрес физического узла.

Замечание!

Адрес физического узла для резервных панелей

У резервной панели должен быть тот же адрес физического узла, что и у назначенной основной панели.

Замечание!

Используемая сеть должна соответствовать следующим минимальным требованиям:

Минимальная пропускная способность: 1 Мбит/с

Максимальная задержка: 250 мс

Замечание!
EN 54
В соответствии со стандартом EN 54 применяются только компоненты, сертифицированные для использования в сетях систем пожарной сигнализации. Внешние RSTP-коммутаторы и медиаконвертеры в сетях Ethernet должны быть установлены в корпусах панелей. Установка за пределами корпуса панели нарушает требования EN 54.

Замечание!
Резервная панель — EN 54-2
Согласно EN 54-2, для каждой панели можно подключить не более 512 тревожных точек. Если это число превышено, при проектировании панели необходимо обеспечить резервирование.
Кроме того, если панель выполняет функции интерфейса с кольцевой подсетью CAN и в кольцевой подсети подключено более 512 тревожных точек, необходимо спроектировать панель с резервированием. RSTP-коммутатор, подключающий 2 кольца, обеспечивает резервирование.

Замечание!
Число логических точек
К автономной панели можно подключить до 4096 логических точек (несмотря на обеспеченное резервирование). Если панель включена в сеть, можно подключить не более 2048 логических точек.

Замечание!
Убедитесь, что назначенный панели адрес физического узла совпадает с соответствующим адресом в программе конфигурирования. Этот адрес отвечает за назначение последнего октета IP-адреса в стандартных настройках.
Активируйте RSTP как протокол резервирования и примите стандартные значения по умолчанию.

Стандартные настройки Ethernet для пожарной панели
В стандартных настройках пожарной панели ПО конфигурирования FSP-5000-RPS и контроллер используют назначенный адрес физического узла в качестве последнего октета IP-адреса.

Замечание!
Работоспособность сети требует правильной настройки адреса физического узла в контроллерах панели и ПО конфигурирования FSP-5000-RPS.

Замечание!
В контроллере панели можно отдельно активировать использование резервирования Ethernet.

- Параметры IP
  - IP-адрес 192.168.1.x
    Последняя цифра IP-адреса в стандартных настройках всегда идентична адресу физического узла, заданному в контроллере панели.
  - Маска сети 255.255.255.0

  - Шлюз 192.168.1.254
  - Адрес многоадресной рассылки 239.192.0.1
  - Номер порта 25001–25008 (можно задать только первый порт; всегда используются 8 последовательных портов)
- Параметры RSTP (настройки по умолчанию)
  - Bridge Priority 32768
  - Hello Time 2
  - Max. Age 20
  - Forward Delay 15

Замечание!
Стандартные настройки конфигурации IP можно использовать в сетях не более чем с 20 RSTP-коммутаторами.
Для сетей, в которых используется более 20 RSTP-коммутаторов, требуются дополнительные настройки в соответствии с топологией. Для этого требуется глубокое знание сетей.

Настройки для кольцевых сетей с более чем 20 RSTP-коммутаторами
Если в сети больше 20 RSTP-коммутаторов, в контроллере панели и программе конфигурирования требуется настроить параметры RSTP. Контроллеры панели, удаленные клавиатуры и подключенные внешние RSTP-коммутаторы считаются RSTP-коммутаторами. Резервные контроллеры панели не считаются RSTP-коммутаторами, так как находящийся в них коммутатор не работает как RSTP-коммутатор.

- Параметры RSTP
  - Сохранить Bridge Priority 32768
  - Сохранить Hello Time 2
  - Изменить Max. Age с 20 на 40
  - Изменить Forward Delay с 15 на 25

Параметры
- В кольце можно использовать не более 32 узлов.
- Диаметр сети не должен превышать 32, см. раздел *Диаметр сети, Страница 21*.
- Коммутаторы Ethernet не должны использоваться вне корпусов панелей.
- Преобразователи среды не должны использоваться вне корпусов панелей.

Характеристики
- Сеть соответствует EN 54.
- В сети используется RSTP.

4.1 Кольцо CAN

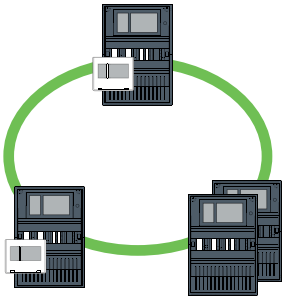


Рис. 4.1: Кольцо CAN

4.2 Кольцо Ethernet

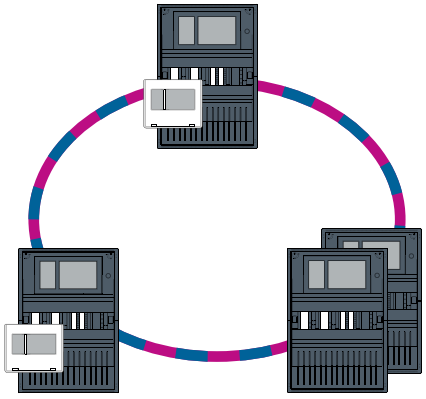


Рис. 4.2: Кольцо Ethernet

4.3 Двойное кольцо Ethernet/CAN

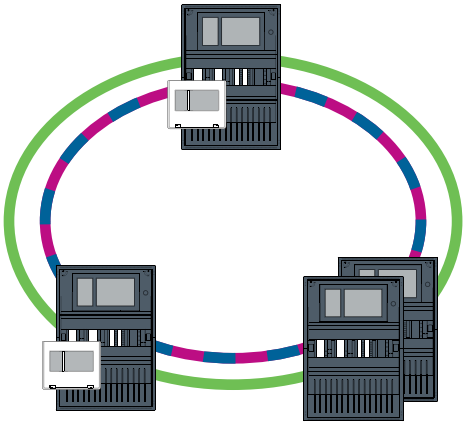


Рис. 4.3: Двойное кольцо Ethernet и CAN

4.4 Кольцо CAN с сегментами Ethernet

Главная топология — это кольцо CAN. Если расстояние между двумя узлами превышает 1000 м, для покрытия расстояния можно использовать подключение Ethernet FX.

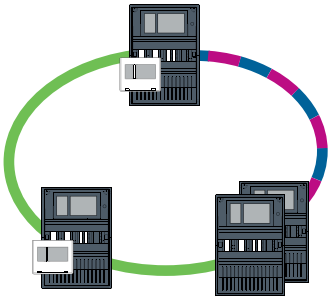


Рис. 4.4: Кольцо CAN с сегментами Ethernet

4.5 Магистраль Ethernet с кольцевыми подсетями (Ethernet/CAN)

Ethernet-магистраль подключается ко всем кольцевым подсетям и, следовательно, является основной областью подключения с высокой скоростью передачи данных. RSTP-коммутаторы в магистрали по умолчанию не являются коммутаторами высшего уровня. Обратите внимание, что в случае этой топологии требуется определить диаметр

сети. Контроллеры панели, удаленные клавиатуры и подключенные внешние RSTP-коммутаторы считаются RSTP-коммутаторами. Объединенные в сеть CAN панели не учитываются при определении диаметра сети.
Настройки колец с более 20 RSTP-коммутаторами см. в разделе *Настройки для кольцевых сетей с более чем 20 RSTP-коммутаторами, Страница 16*.

Замечание!
Эта топология требует дополнительной настройки всех RSTP-коммутаторов в магистрали. Поэтому требуется более глубокое знание сетей.

Замечание!
Если панель выступает как интерфейс с кольцевой подсетью CAN, в соответствии с EN 54-2 она также требует резервирования, если в подсети подключено более 512 тревожных точек.
Это ограничение не применимо в кольцевой подсети Ethernet, так как функцию резервирования выполняют подключенные к данным двум кольцевым шлейфам коммутаторы.

Дополнительные параметры
Центральное кольцо следует использовать как магистраль. Центральное кольцо необходимо подключить к сети с помощью Ethernet.

Замечание!
Для всех RSTP-коммутаторов в магистрали следует задать более высокий RSTP-приоритет, чем в подсетях. В результате корневой мост RSTP всегда останется в магистрали, даже в случае отказа.
RSTP-коммутаторы для кольцевых подсетей — часть магистрали!
В магистрали используйте RSTP-приоритет 16384.

Замечание!
Чем меньше заданное значение, тем выше RSTP-приоритет.

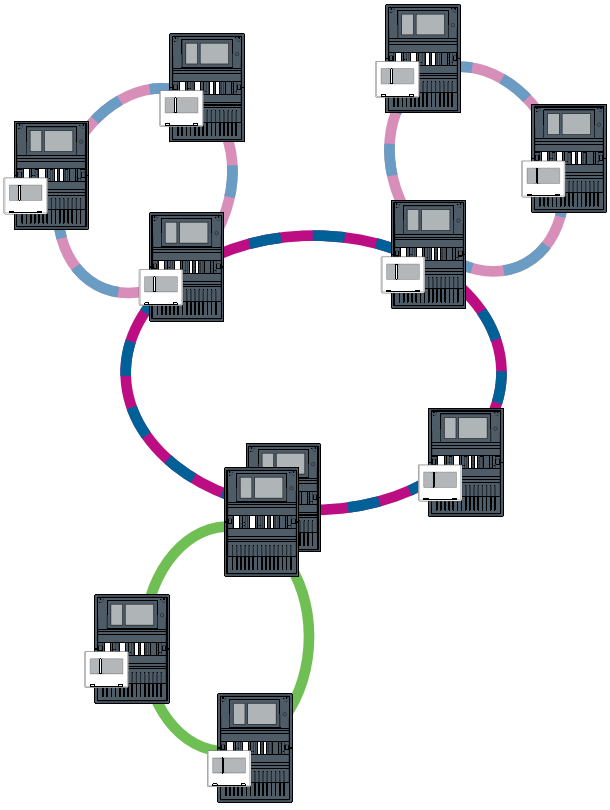


Рис. 4.5: Магистраль Ethernet с кольцевыми подсетями

4.6 Подключение колец Ethernet

Замечание!
Эта топология требует дополнительной настройки всех RSTP-коммутаторов в магистрали. Поэтому требуется более глубокое знание сетей.

Дополнительные параметры
Эта топология — специальный случай магистрали Ethernet с кольцевыми подсетями. См. раздел Магистраль Ethernet с кольцевыми подсетями (Ethernet/CAN). Одну из двух кольцевых сетей необходимо использовать как магистраль.

Замечание!
Для всех панелей и коммутаторов в магистрали следует задать более высокий RSTP-приоритет, чем в подсетях. В результате корневой мост RSTP всегда останется в магистрали, даже в случае отказа.
Коммутаторы для подключения двух кольцевых подсетей — часть магистрали!
В магистрали используйте RSTP-приоритет 16384.

Замечание!
Чем меньше заданное значение, тем выше RSTP-приоритет.

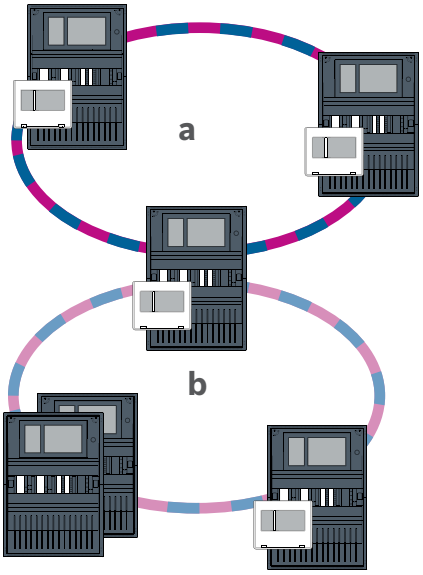


Рис. 4.6: Подключение кольцевого шлейфа Ethernet через панель без резервирования

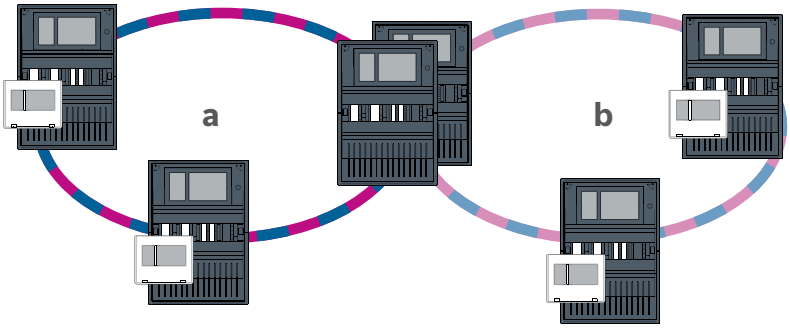


Рис. 4.7: Подключение кольцевого шлейфа Ethernet через резервную панель

5 Сеть Ethernet

В сети сетевые подключения Ethernet постоянно контролируются. В случае разрыва соединения регистрируется обрыв. Также обнаруживаются восстановления соединений. Сетевая диагностика панели всегда показывает MAC-адреса хостов, подключенных через сеть.

MAC-адреса

Каждый контроллер панели предоставляет следующие MAC-адреса для сетевого подключения.

- MAC-адрес для хоста
- MAC-адрес для определения порта ETH1
- MAC-адрес для определения порта ETH2

В зависимости от типа контроллера панели:

- MAC-адрес для определения порта ETH3
- MAC-адрес для определения порта ETH4

Правила использования 4 портов Ethernet

Если панель имеет 4 порта Ethernet, примените следующие правила в указанном порядке. Bosch поддерживает сети, построенные в соответствии со следующими правилами.

1. Для подключения панелей необходимо использовать ETH1 и ETH2. Для подключения панелей должен использоваться только внешний RSTP-коммутатор на ETH1 или ETH2.
2. Для подключения системы управления зданием, системы речевого и аварийного оповещения или иерархической панели необходимо использовать ETH3. Можно подключить внешний RSTP-коммутатор, который не должен использоваться для подключения панелей.
3. Для Remote Services необходимо использовать ETH4. Если подключение к Remote Services не требуется, то ETH4 можно использовать для подключения системы управления зданием, системы речевого и аварийного оповещения или иерархической панели.
4. При отсутствии сетевого подключения панелей через ETH1 и ETH2, каждая из них может быть использована для подключения системы управления зданием, системы речевого и аварийного оповещения или иерархической панели.

5.1 Протоколы

SNMP

SNMP используется для контроля и управления сетевыми компонентами. С этой целью можно считывать и изменять параметры узлов сети. Для этого потребуется соответствующее программное обеспечение для управления сетью (например, Hirschmann HiVision).

Замечание!

В сети используется фиксированная строка сообщества SNMP: PUBLIC

Обратите внимание, что серия AVENAR panel пока не поддерживает протокол SNMP.

LLDP

LLDP — базовый протокол, стандартизованный институтом IEEE. Он используется для обмена информацией о сети между соседними устройствами. Эта информация

– предоставляется как часть SNMP-данных и
– отображается на контроллере панели как часть сетевых диагностических данных.

RSTP

RSTP — сетевой протокол, стандартизованный институтом IEEE. RSTP обеспечивает отсутствие колец в сетях. Резервные пути в сети обнаруживаются и отключаются или включаются при необходимости (в случае потери соединения).
В сети этот протокол используется именно в этих целях.
Переход на эту топологию из-за отказа соединения автоматически отменяется при восстановления соединения.

5.2 Диаметр сети

Диаметр Ethernet-сетей панелей RSTP не должен превышать 32.

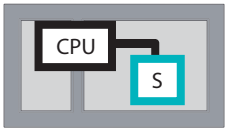
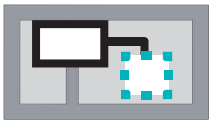
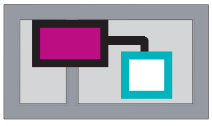
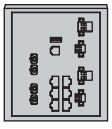
Описание

Диаметр сети соответствует количеству RSTP-коммутаторов на самом длинном участке без петель между любыми двумя конечными точками в сети.
В отношении Ethernet-сети панелей RSTP следует учитывать следующее:

– Каждый контроллер панели содержит конечную точку и внутренний RSTP-коммутатор.

- Сочетание контроллера панели и резервного контроллера панели считается одним RSTP-коммутатором.
- Преобразователи среды не считаются RSTP-коммутаторами.
- В самую длинный участок не могут входить CAN-подключения.
- Диаметр определяется без учета систем управления зданием.

Ключ

	Центральный процессор в контроллере панели или на удаленной клавиатуре.
	Внутренний коммутатор RSTP в контроллере панели или на удаленной клавиатуре.
	Контроллер панели или удаленная клавиатура с центральным процессором и внутренним коммутатором RSTP.
	Резервный контроллер панели с центральным процессором и внутренним коммутатором RSTP.
	Контроллер панели или удаленная клавиатура Начальная или конечная точка для определения диаметра сети в примерах.
	Коммутатор Ethernet в качестве внешнего RSTP-коммутатора (или универсальный коммутатор Ethernet MM)

Две связанные панели образуют минимально возможное кольцо. Диаметр этой сети равен 2, так как внутренние коммутаторы RSTP расположены между конечными точками.

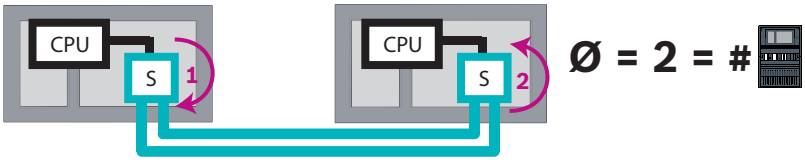


Рис. 5.1: Сетевой диаметр кольца с 2 панелями

В кольце панелей без внешних коммутаторов RSTP диаметр сети соответствует числу установленных панелей.

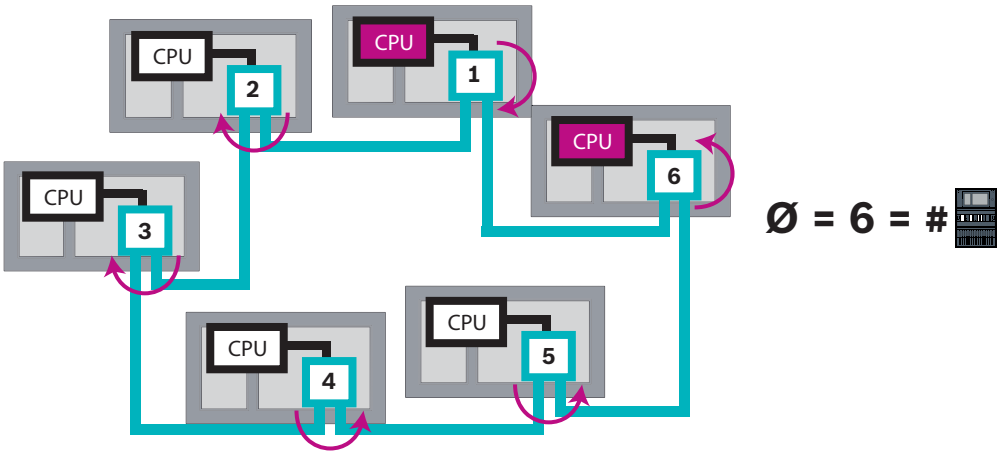


Рис. 5.2: Сетевой диаметр кольца с 6 панелями

Если магистраль и кольцевые подсети подключены друг к другу с помощью коммутаторов Ethernet, необходимо также учитывать внешние коммутаторы RSTP.

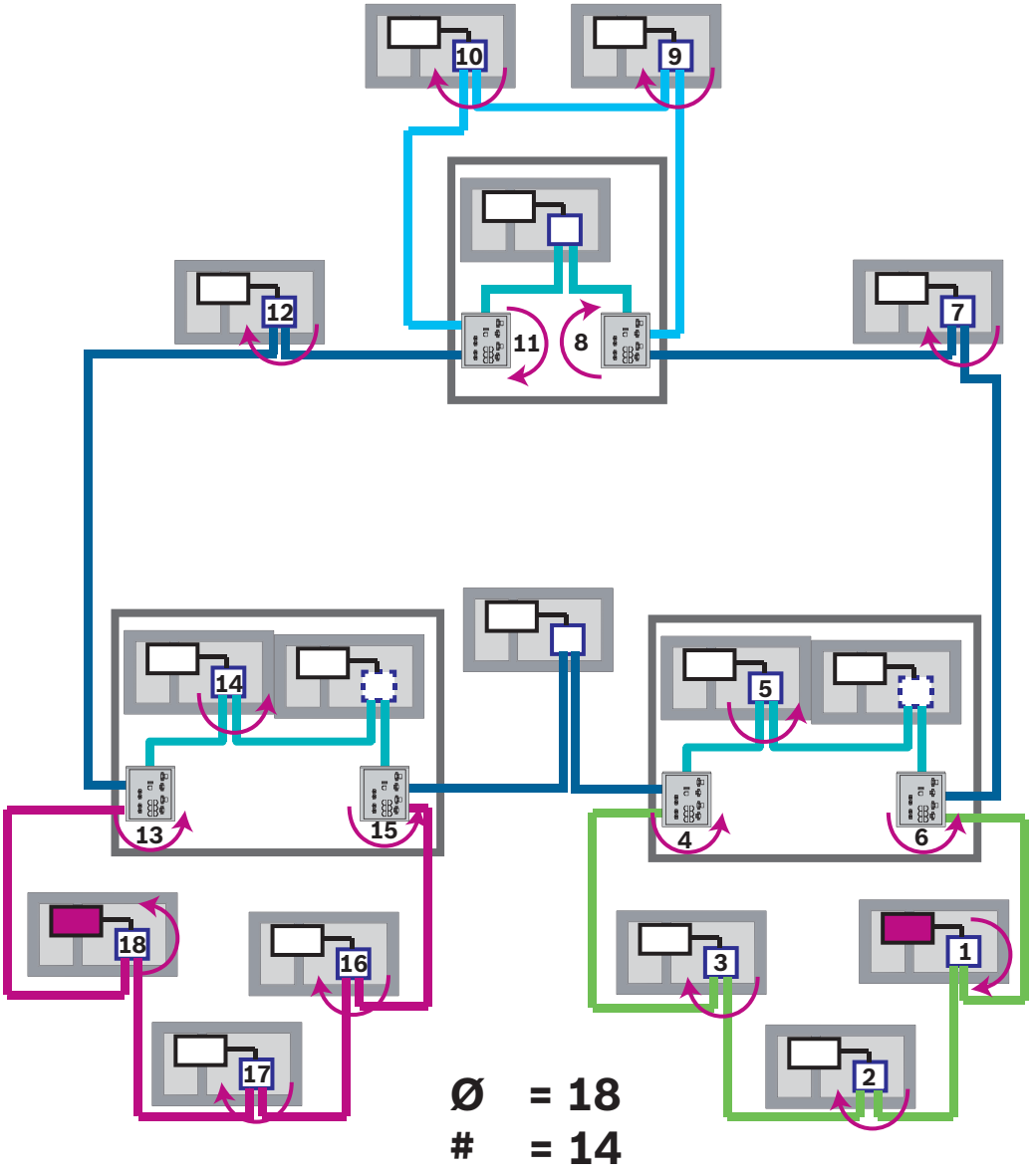


Рис. 5.3: Сетевой диаметр магистрали с кольцевыми подсетями

На рисунке показано, что для этого диаметра требуется использовать самый длинный путь.

5.3 Используемые кабели

Для организации сетей Ethernet следует использовать только следующие кабели. Использование других кабелей противоречит стандартам безопасности в директивах ЕС.

– Кабель Ethernet
  Экранированный Ethernet-кабель CAT 5e или выше.
  Обратите внимание на минимальные радиусы сгиба, указанные в технических характеристиках кабеля.
– Оптоволоконный кабель
  Многомодовый: оптоволоконный экранированный кабель Ethernet, дуплекс I-VH2G 50/125µ или I-VH2G 62.5/125µ, заглушка SC.
  Одномодовый: оптоволоконный экранированный Ethernet-кабель, дуплекс I-VH2E 9/125µ, заглушка SC.
  Обратите внимание на минимальные радиусы сгиба, указанные в технических характеристиках кабеля.

Замечание!
Длина кабеля TX
Все IP-подключения должны осуществляться напрямую или через медиаконвертеры, утвержденные Bosch. Длина кабеля TX между узлами должна быть менее 100 м.

Замечание!
VdS 2540 - Сеть Ethernet
Применительно к Ethernet-сетей панелей следует учитывать, что для установки в Германии, где требуется соответствие стандарту VdS 2540, для всех путей передачи данных должен использоваться оптоволоконный кабель. Единственным исключением является корпус.

5.4 Создание или изменение сети Ethernet

Существует несколько процедур создания Ethernet-сети панелей пожарной сигнализации. Две описанные ниже процедуры отличаются по размеру систем и числу выполняемых параллельно задач по монтажу и настройке.

Правила использования 4 портов Ethernet
Если панель имеет 4 порта Ethernet, примените следующие правила в указанном порядке. Bosch поддерживает сети, построенные в соответствии со следующими правилами.

1. Для подключения панелей необходимо использовать ETH1 и ETH2. Для подключения панелей должен использоваться только внешний RSTP-коммутатор на ETH1 или ETH2.
2. Для подключения системы управления зданием, системы речевого и аварийного оповещения или иерархической панели необходимо использовать ETH3. Можно подключить внешний RSTP-коммутатор, который не должен использоваться для подключения панелей.
3. Для Remote Services необходимо использовать ETH4. Если подключение к Remote Services не требуется, то ETH4 можно использовать для подключения системы управления зданием, системы речевого и аварийного оповещения или иерархической панели.

4. При отсутствии сетевого подключения панелей через ETH1 и ETH2, каждая из них может быть использована для подключения системы управления зданием, системы речевого и аварийного оповещения или иерархической панели.

Создание Ethernet-сети (для небольших проектов)

Эта процедура подходит для проектов с небольшим числом инженеров, параллельно работающих над установкой системы пожарной сигнализации.

1. Создайте план сети.
2. Создайте сеть в FSP-5000-RPS и настройте параметры сети.
3. Распечатайте информацию о сети или сохраните ее на ноутбуке.
4. Установите панели управления и сетевые кабели, затем подключите их к сети.
5. Прямо с блока управления настройте параметры сети для каждой панели управления в соответствии с распечаткой.
6. Выполните сброс каждой панели управления в сети для активации конфигурации сети.
7. Подключите компьютер к панели управления в сети с помощью программного обеспечения для программирования FSP-5000-RPS. Загрузите эту конфигурацию на все панели управления в сети с помощью этой панели управления. Резервные панели используют конфигурацию основной панели.
8. Выполните сброс ожидающих сообщений об ошибках. Исправьте все ошибки.

Сначала настройте параметры сети на панелях управления. Благодаря этому вы сможете программировать другие панели управления в сети с помощью одной панели управления.

Создание сети Ethernet (для средних и крупных проектов)

Эта процедура подходит для проектов со значительным числом задач, выполняемых параллельно несколькими группами. Так как многие задачи, выполняемые во время установки и настройки, включают перезапуск панели управления пожарной тревогой, в этой процедуре сеть запускается на более поздней стадии.

1. Создайте план сети.
2. Создайте конфигурацию сети без периферийных устройств с помощью FSP-5000-RPS.
3. Распечатайте информацию о сети или сохраните ее на ноутбуке.
4. Установите сетевые кабели и проверьте отдельные участки или кольцевые шлейфы.
5. Установите панели и введите их в эксплуатацию как автономные панели.
6. Установите периферийные устройства на панелях.
7. Настройте каждую панель с помощью FSP-5000-RPS.
8. Убедитесь, что все панели работают правильно.
9. Поочередно введите в эксплуатацию отдельные кольцевые шлейфы сети в соответствии с топологией.

   Начните с магистрали.

   - Создайте конфигурацию для магистрали в FSP-5000-RPS. Импортируйте все необходимые конфигурации панелей. Настройте параметры сети и распечатайте их.
   - Подключите все панели к сети.
   - Прямо с контроллера панели настройте параметры сети для каждой панели управления в соответствии с распечаткой.
   - Выполните сброс каждой панели управления для загрузки конфигурации сети.
   - Проверьте доступность соседних панелей с помощью команды PING для проверки сети.
   - Введите в эксплуатацию всю магистраль и исправьте все ошибки.

Введите в эксплуатацию кольцевые подсети, как показано в примере магистрали.

Добавление панели в сеть

1. Измените конфигурацию сети в FSP-5000-RPS.
2. Распечатайте информацию о сети или сохраните ее на ноутбуке.
3. Проложите кабели панели управления и сети и подключите их к сети.
4. Прямо с блока управления настройте параметры сети для каждой панели управления в соответствии с распечаткой.
5. Выполните сброс панели и смежных с ней панелей, чтобы активировать конфигурацию сети.

Удаление панели из сети

1. Измените конфигурацию сети в FSP-5000-RPS.
2. Распечатайте информацию о сети или сохраните ее на ноутбуке.
3. Прямо с блока управления настройте параметры сети для смежных панелей управления в соответствии с распечаткой.
4. Отключите панель и источник питания (сеть и аккумулятор), прежде чем извлекать панель из сети.
5. Выполните сброс смежных панелей, чтобы активировать конфигурацию сети.

6 Сеть CAN

Кольцевая топология

В кольцевой топологии кабель CAN всегда прокладывается от клеммы CAN1 к клемме CAN2 [CAN1 ⇒ CAN2]. Длина кабеля зависит от его поперечного сечения.

Подключение CAN

Соединение CAN является двухпроводным (CAN-H и CAN-L). Для двухжильного соединения подключите CAN-H к CAN-H, а CAN-L – к CAN-L. В исключительных случаях может потребоваться трехжильное соединение (CAN-H, CAN-L и CAN-GND), например, при высокой нагрузке EMC или значительной разнице потенциала земли. Для трехжильного соединения подключите CAN-H к CAN-H, CAN-L к CAN-L, а CAN-GND – к CAN-GND. Экран кабеля CAN подключается к металлическому корпусу панели только с одной стороны.

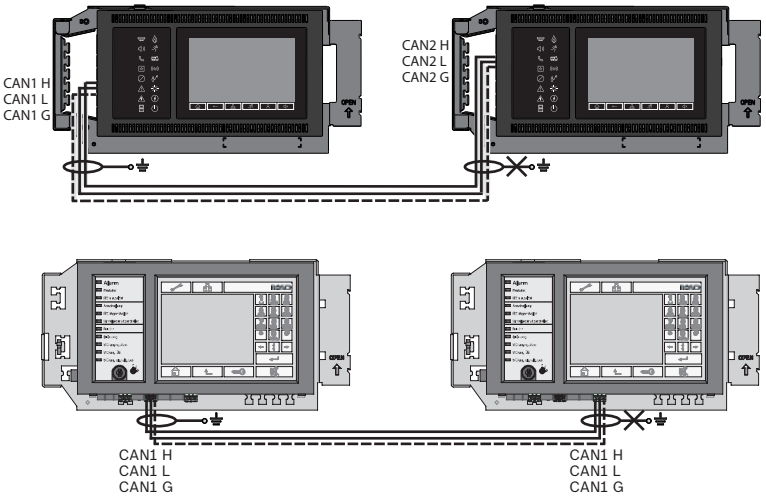


Рис. 6.1: Подключение CAN (вверху: AVENAR, внизу: FPA)

Длина кабеля для сетевого подключения

Максимально допустимая длина кабеля зависит от контурного сопротивления используемого кабеля и числа узлов, обменивающихся данными.

Пример: красный кабель пожарной сигнализацииJ-Y (St) Y 2 x 2 x 0,8 mm позволяет соединить два узла, расстояние между которыми не превышает 800 m.

Замечание!
Расстояние между двумя узлами в кольцевой топологии можно определить, считав нужное значение в двух узлах диаграммы.

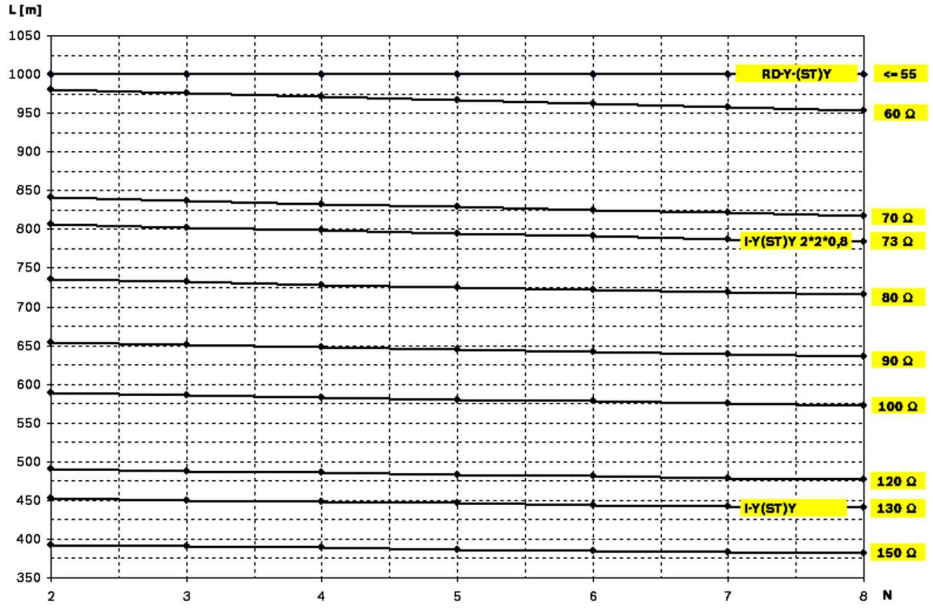


Рис. 6.2: Сеть CAN: допустимая длина кабеля в зависимости от числа узлов и сопротивления кабеля

L = длина кабеля в метрах

N = число узлов

6.1 Создание или изменение сети CAN

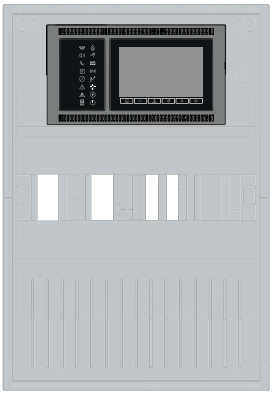
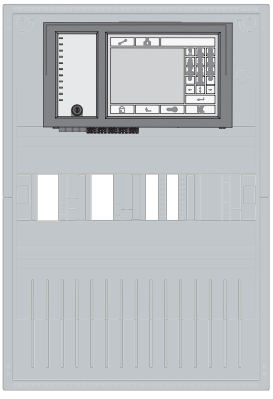
Эта процедура подходит для проектов с небольшим числом инженеров, параллельно работающих над установкой системы пожарной сигнализации.

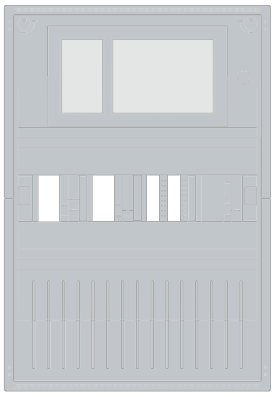
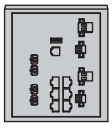
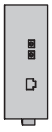
Процедура создания сети CAN

1. Создайте план сети.
2. Создайте сеть в FSP-5000-RPS.
3. Распечатайте информацию о сети или сохраните ее на ноутбуке.
4. Установите панели управления и подключите их к сети с помощью кабелей CAN.
5. Подключите компьютер к панели управления в сети с помощью программного обеспечения для программирования FSP-5000-RPS. Загрузите эту конфигурацию на все панели управления в сети с помощью этой панели управления. Резервные панели используют конфигурацию основной панели.
6. Выполните сброс ожидающих сообщений об ошибках. Исправьте все ошибки.

7 Схема сетевого подключения Ethernet и CAN

Для создания сетей панелей, соответствующих представленным топологиям, и подключения служб необходимо воспользоваться описанным в этом документе сетевым шаблоном.

Значок	Описание
	Кабель Ethernet TX (медный), длина кабеля TX между узлами < 100 м
	Кабель Ethernet FX (оптоволоконный)
	Кабель Ethernet TX или FX, длина кабеля TX между узлами < 100 м
	Кабель CAN
	Корпус Примечание. Для упрощения представления различных схем сетевого подключения на рисунках в этой главе все панели обозначаются малыми корпусами панелей. Малый корпус может **не** обеспечивать достаточное пространство для отображенных коммутаторов, медиаконвертеров и шлюзов. Используйте средство Safety Systems Designer для подбора правильного количества и размера корпусов для установки заказываемого оборудования.
	AVENAR panel
	FPA

Значок	Описание
	AVENAR panel или FPA
	Коммутатор Ethernet в качестве внешнего RSTP-коммутатора (или универсальный коммутатор Ethernet MM)
	Медиаконвертер
	Защищенный сетевой шлюз для Remote Services
	Подключение к системе управления зданием, система речевого и аварийного оповещения или иерархической панели

7.1 Ethernet-сеть панелей

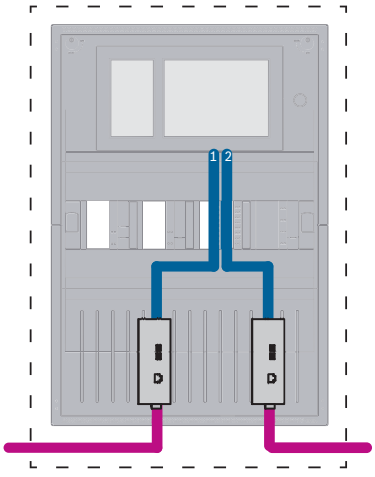


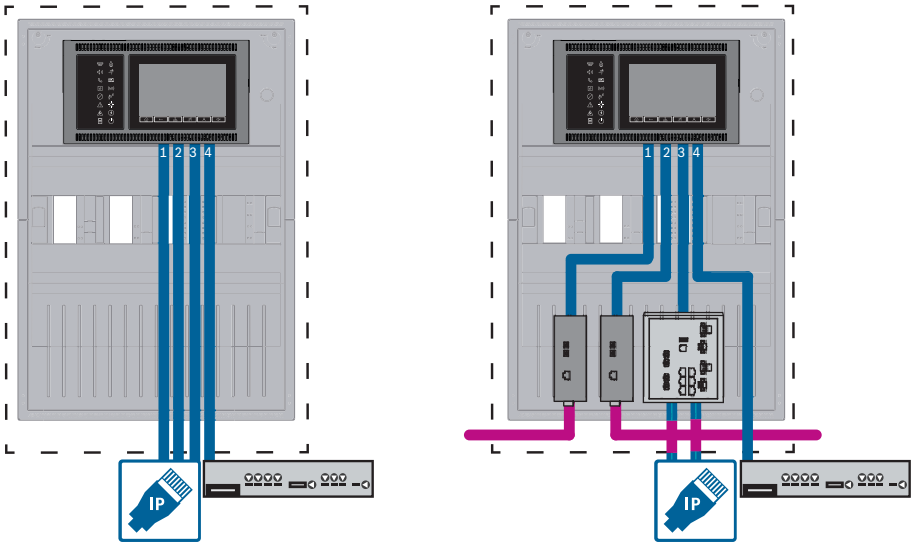
Рис. 7.1: Ethernet-сеть панелей

Для диапазонов более 100 м требуется использовать расширение диапазона с преобразователями среды. Для диапазонов менее 100 м преобразователи среды могут не потребоваться.

7.2 CAN-сеть панелей

Рис. 7.2: CAN-сеть панелей

7.3 Подключение служб к панели



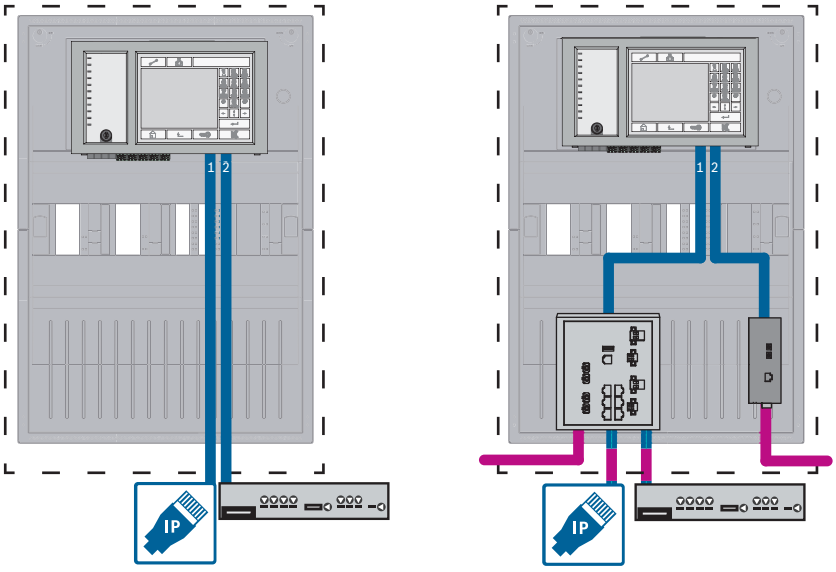


Рис. 7.3: Левая сторона: без сети панелей, правая сторона: с сетью панелей

Коммутатор Ethernet необходим, только если к панели подключены более двух служб. Для диапазонов более 100 м требуется использовать расширение диапазона с преобразователями среды. Для диапазонов менее 100 м преобразователи среды могут не потребоваться.

7.4 Ethernet-сеть панелей с резервными панелями

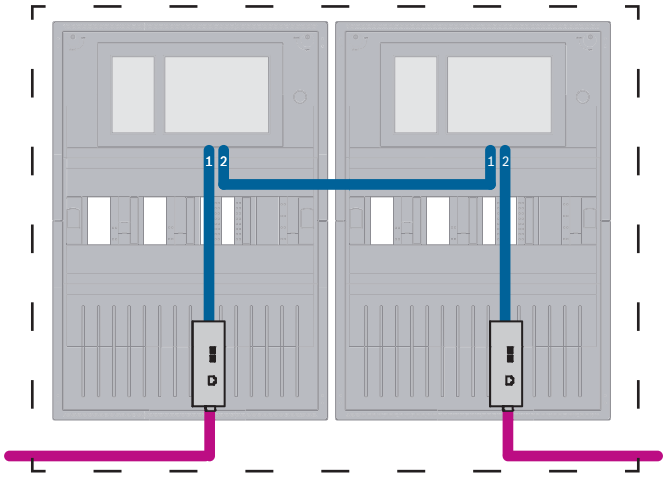


Рис. 7.4: Ethernet-сеть панелей с резервными панелями

Для диапазонов более 100 м требуется использовать расширение диапазона с преобразователями среды. Для диапазонов менее 100 м преобразователи среды могут не потребоваться.

7.5 CAN-сеть панелей с резервными панелями

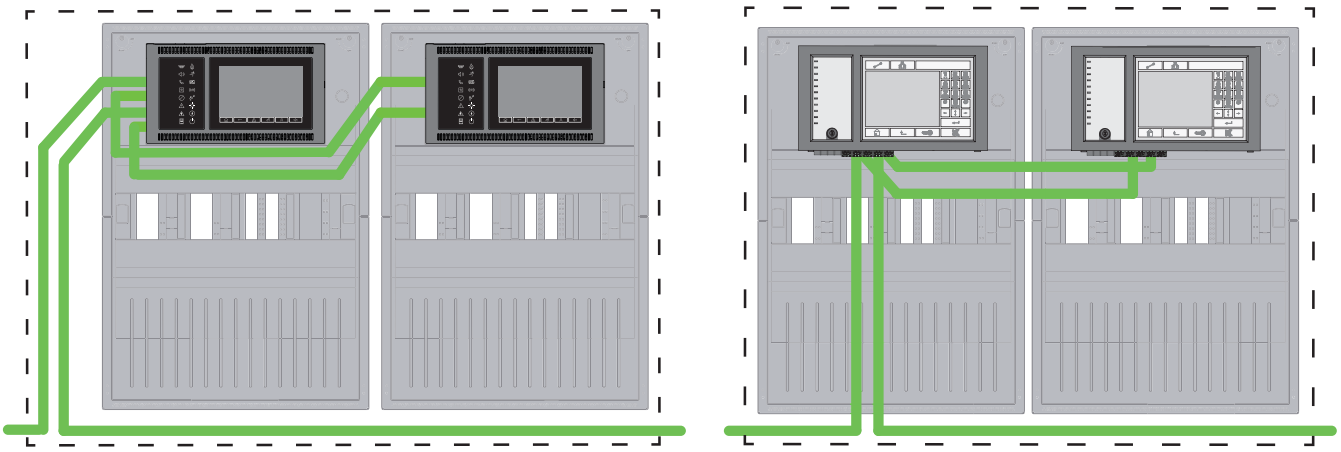


Рис. 7.5: CAN-сеть панелей с резервными панелями

7.6 Сеть панелей с двумя кольцами Ethernet

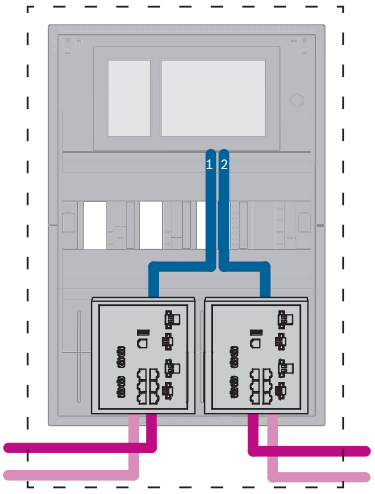


Рис. 7.6: Подключение сетей Ethernet

7.7 Сеть панелей с двумя кольцами Ethernet и резервными панелями

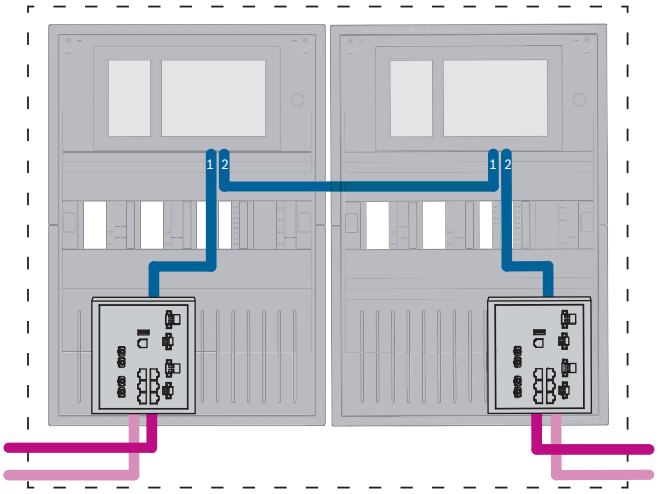


Рис. 7.7: Подключение Ethernet-сетей с резервными панелями

7.8 Подключение Ethernet- и CAN-среды с резервными панелями

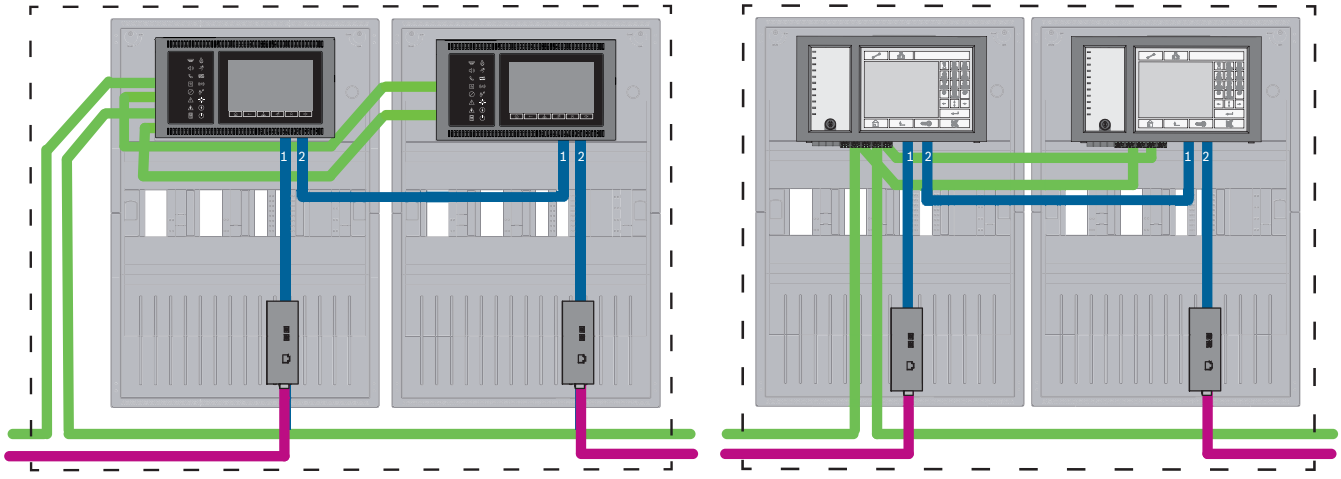


Рис. 7.8: Подключение Ethernet- и CAN-среды с резервными панелями

Для диапазонов более 100 м требуется использовать расширение диапазона с преобразователями среды. Для диапазонов менее 100 м преобразователи среды могут не потребоваться.

7.9 Подключение удаленных служб к резервным панелям

Есть возможность подключения защищенного сетевого шлюза к резервной FPA или резервной AVENAR panel. По указанным ниже причинам рассмотрите возможность подключения защищенного сетевого шлюза не к резервной AVENAR panel, а к AVENAR panel без резервирования:

- Процедура является временным решением.
- При подключении к системе управления зданием необходимо использовать и настроить порт ETH3 контроллера резервной панели.

7.9.1 Резервная панель AVENAR

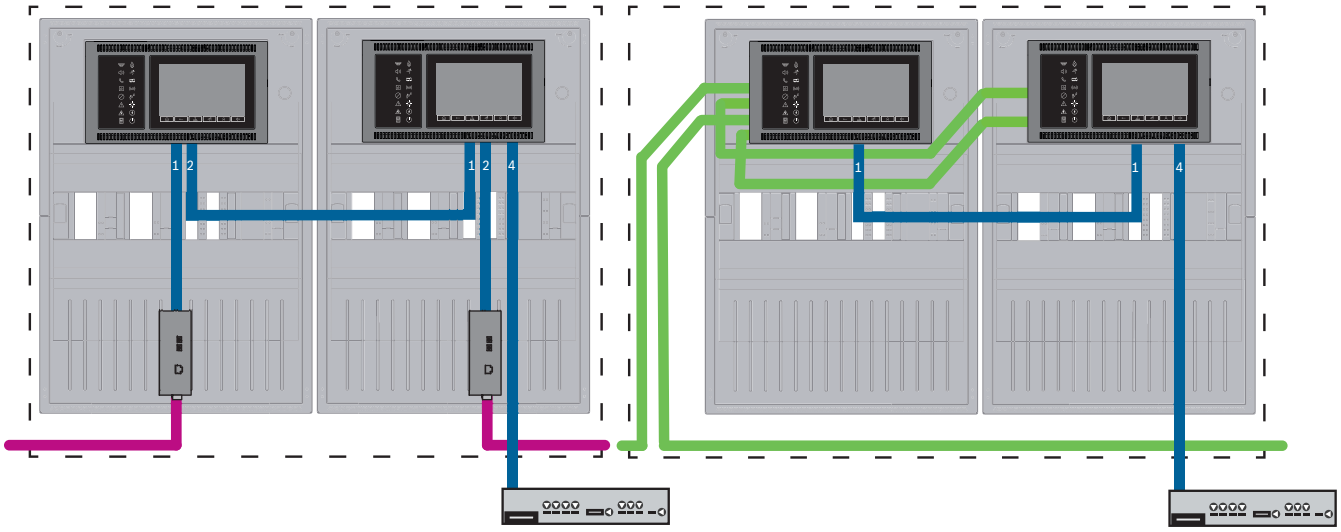


Рис. 7.9: Левая сторона: в сети Ethernet; правая сторона: в сети CAN

Для диапазонов более 100 м требуется использовать расширение диапазона с преобразователями среды. Для диапазонов менее 100 м преобразователи среды могут не потребоваться.

Процедура

1. Подключите защищенный сетевой шлюз к порту ETH4 контроллера резервной панели.
2. В сети CAN необходимо подключить кабель Ethernet от порта ETH1 к порту ETH1 контроллера резервной панели. Настройте параметры ETH1 в окне FSP-5000-RPS **Сетевой интерфейс**–**Ethernet**:
   - Для **Тип линии** выберите **Канал связи**
   - Если номер строки больше, чем 0, в **Подключено к линии №**, то соединение защищено.
3. В сети CAN или Ethernet настройте параметры ETH4 в окне FSP-5000-RPS **Сетевой интерфейс**–**Ethernet**:
   - Введите 0 в **Подключено к линии №**.
   - Отметьте **Использовать порт**.

7.9.2 Резервный FPA

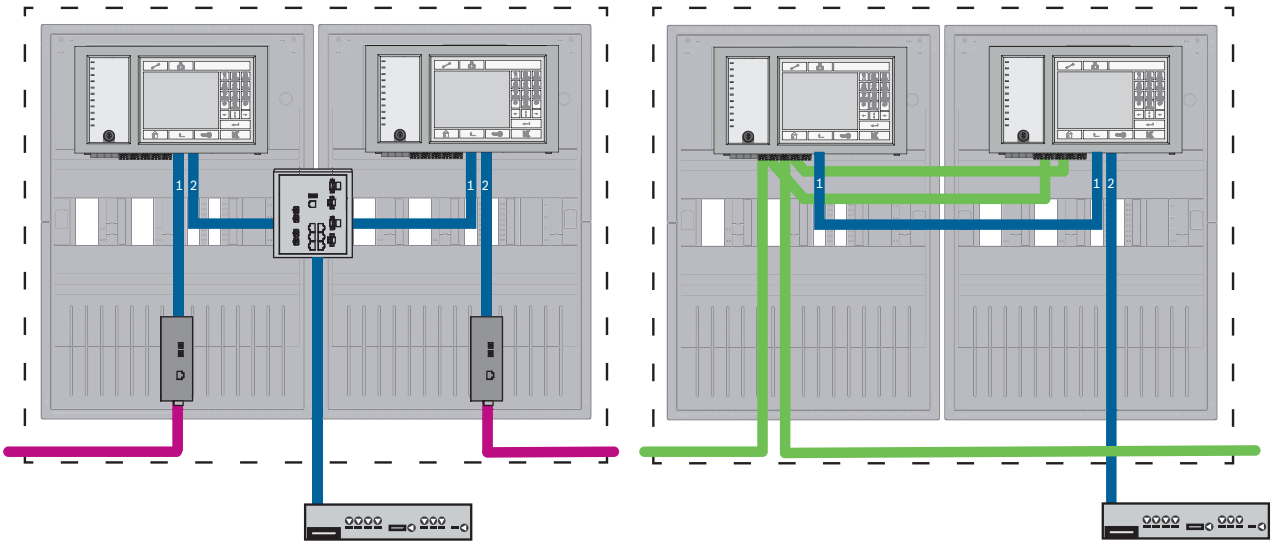


Рис. 7.10: Левая сторона: в сети Ethernet; правая сторона: в сети CAN

Для диапазонов более 100 м требуется использовать расширение диапазона с преобразователями среды. Для диапазонов менее 100 м преобразователи среды могут не потребоваться.

Процедура в сети CAN

1. Подключите защищенный сетевой шлюз к порту ETH2 контроллера резервной панели.
2. В сети CAN необходимо подключить кабель Ethernet от порта ETH1 к порту ETH1 контроллера резервной панели. Настройте параметры ETH1 в окне FSP-5000-RPS **Сетевой интерфейс**–**Ethernet**:
   - Для **Тип линии** выберите **Канал связи**
   - Если номер строки больше, чем 0, в **Подключено к линии №**, то соединение защищено.
3. Настройте параметры ETH2 в окне FSP-5000-RPS **Сетевой интерфейс**–**Ethernet**:
   - Введите 0 в **Подключено к линии №**.
   - Отметьте **Использовать порт**.

7.10 Подключение служб безопасности жизнедеятельности к резервным панелям

Подключение службы безопасности жизнедеятельности должно осуществляться к панели AVENAR panel без резервирования:

- Временное решение для удаленных служб не подходит для подключения служб, связанных с безопасностью жизнедеятельности, к системам речевого и аварийного оповещения (VAS over IP) или к иерархической панели. Необходимо установить сертифицированный коммутатор EN 54, подключенный к контроллерам главной и резервной панелей.

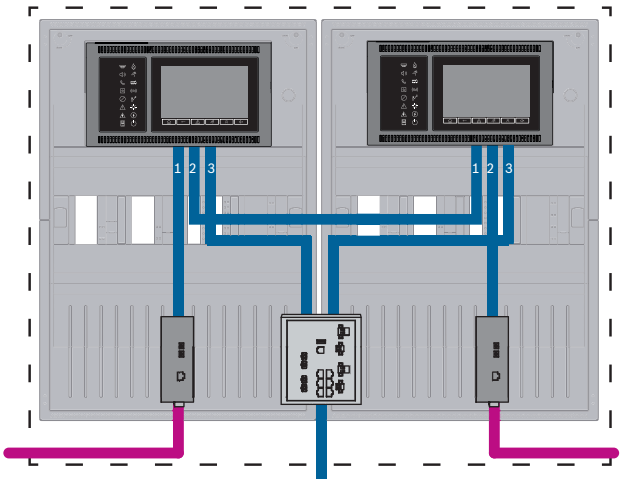


Рис. 7.11: Интерфейс для подключения VAS и иерархической панели к резервной панели AVENAR

8 Службы Remote Services

Remote Services включают следующие службы:

– Remote Alert
– Remote Maintenance

Предварительным условием для Remote Alert и Remote Maintenance является Remote Connect.

Замечание!
Хотя Remote Connect поддерживает подключение к сети панелей по сети Ethernet или CAN, функциональность Remote Alert и Remote Maintenance поддерживается, только если для службы предоставлено и настроено подключение Ethernet между панелями.

Замечание!
Ethernet-соединения, используемые только для передачи данных Remote Maintenance, можно реализовать с помощью Ethernet-кабелей или оптоволоконных соединений. Обращайте внимание на максимально допустимую длину кабелей.

Внимание!
Remote Services требуют безопасного IP-подключения. Требуется Bosch Remote Services или подключение к Private Secure Network.
Вместе с сетью Private Secure Network предоставляется IP-сеть на основе подключения DSL с дополнительным беспроводным доступом со стороны панели (EffiLink). Remote Services для Private Secure Network предоставляются только в Германии по соглашению об обслуживании с Bosch BT-IE.

8.1 Требования для использования служб Remote Services

8.1.1 Служба Remote Connect

Remote Connect предоставляет надежное, защищенное подключение к Интернету для удаленного доступа к панели с помощью FSP-5000-RPS. Служба Remote Connect необходима для всех служб Remote Services. Для Remote Connect используйте защищенный сетевой шлюз.

В случае сети панелей одна из панелей в сети должна быть подключена к сетевому шлюзу безопасности. Это подключение должно осуществляться исключительно посредством выделенного Ethernet-соединения. В конфигурации этой панели в FSP-5000-RPS должна быть включена опция Remote Connect.
На следующих схемах показаны:

– топология с подключением контроллеров панели по Ethernet, где сетевой шлюз безопасности подключен к сети с помощью коммутатора Ethernet (обычно MM);
– топология с сетью CAN, где сетевой шлюз безопасности подключен к сети с помощью порта Ethernet.

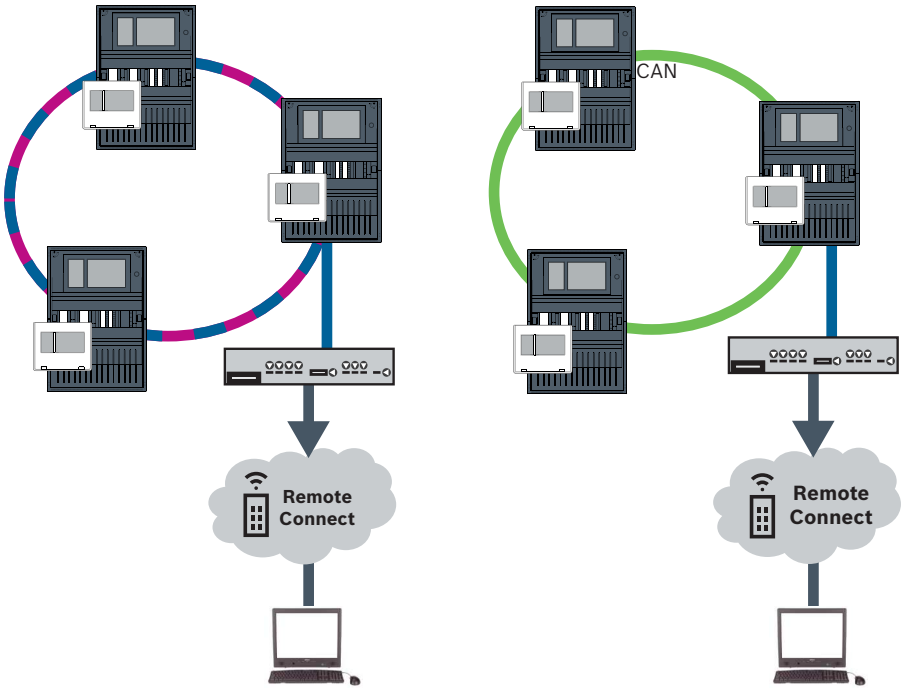


Рис. 8.1: Remote Connect в кольцевой сети Ethernet | Remote Connect в кольцевой сети CAN

Подключите сетевой шлюз безопасности

Для работы Remote Services требуется использовать сетевой шлюз безопасности.

1. Подключите порт WAN сетевого шлюза безопасности к маршрутизатору для Интернета или сети компании, предоставляющей доступ к Интернет.
2. На интернет-маршрутизаторе или в корпоративной сети проверьте доступность следующих протоколов и портов для сетевого шлюза безопасности (требуется для подключения к Remote Services).

Протокол	Порт по умолчанию	Описание
HTTP	80 и 8080	для регистрации Remote Connect и Remote Maintenance
VPN IPsec	UDP 500 и UDP 4500	для Remote Connect

3. Подключите порт LAN1 сетевого шлюза безопасности к назначенному для этого Ethernet-порту контроллера панели, используя входящий в комплект сетевой кабель CAT5 RJ45. Изучите возможные топологии.
4. Подключите сетевой шлюз безопасности к сети питания с напряжением 100 V - 230 V, используя входящий в комплект поставки источник питания.

Светодиод WAN горит (синим), когда установлено подключение к Интернету. Светодиод VPN загорается (синим) вскоре после первого, что свидетельствует об успешном установлении VPN-подключения.

У каждой подключенной панели или сети панелей есть один уникальный System ID.

Замечание!
Для подключения панелей через FX используйте преобразователи среды, утвержденные Bosch.

Чтобы предотвратить передачу относящегося к EN 54-2 многоадресного трафика на маршрутизатор, используйте коммутатор Ethernet (как правило, MM, BPA-ESWEX-RSR20), утвержденный для версии панели 2.8. Активируйте отслеживание IGMP для коммутатора Ethernet, см. соответствующий раздел в главе «Установка» руководства по сетевому подключению.

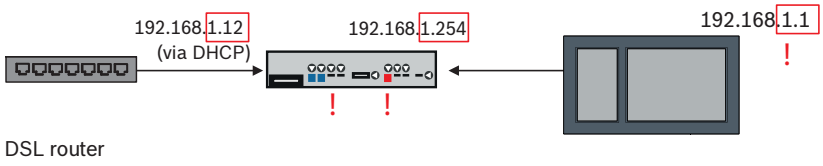
Замечание!
Маршрутизатор Интернета (или сеть компании, которая предоставляет доступ к Интернету), а также защищенный сетевой шлюз должны предоставлять раздельные подсети. Панели сети панелей не следует размещать в подсети маршрутизатора Интернета. Также невозможно перекрытие вложенных сетей.
При перекрытии подсетей их необходимо разделять, изменяя IP-адреса на стороне сети панелей.
Кроме того, необходимо распространить изменения на защищенный сетевой шлюз. Для этого запустите веб-интерфейс в браузере.
- Адрес: https://192.168.1.254
- Имя пользователя: bosch
- Пароль: ipti83

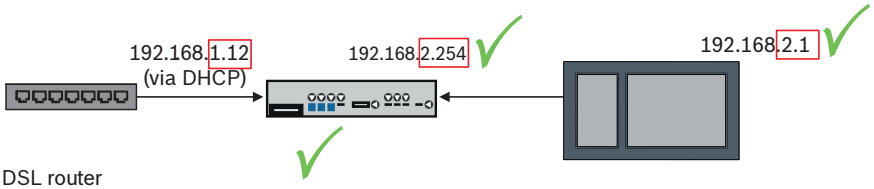
В разделе **Конфигурация** -> **Локальная сеть (LAN)** можно изменить IP-адрес. Обратите внимание, что адрес **Шлюз по умолч.:** в конфигурации контроллера панели должен совпадать с IP-адресом защищенного сетевого шлюза.

Замечание!
Стандарт DIBt запрещает удаленный сброс для восстановления готовности к работе систем управления дверьми с приводом отрывания.

Разделение подсетей (выкл. индикатор VPN)

Подключение защищенного сетевого шлюза к Remote Services не удается в случае перекрытия подсетей (выкл. светодиод VPN). В приведенном ниже примере показана ситуация, когда защищенный сетевой шлюз и контроллер панели находятся в том же адресном диапазоне, что и DSL-маршрутизатор.





Защищенный сетевой шлюз однозначно обнаруживает наложение подсетей: светодиодный индикатор Alarm мигает постоянно.

Разделение подсетей осуществляется через третий октетIP-адреса. IP-адрес меняется в сети панели. После изменения IP-адреса необходимо распространить изменения на защищенный сетевой шлюз. Для этого запустите веб-интерфейс в браузере.

- Адрес: https://192.168.1.254
- Имя пользователя: bosch
- Пароль: ipti83

В разделе **Конфигурация** -> **Локальная сеть (LAN)** можно изменить IP-адрес. Обратите внимание, что адрес **Шлюз по умолч.:** в конфигурации контроллера панели должен совпадать с IP-адресом защищенного сетевого шлюза.

8.1.2 Fire System Explorer

Для использования служб Remote Services необходимо быть пользователем клиента Fire System Explorer (FSE). Один уникальный идентификатор Remote ID должен представлять одну компанию.

Замечание!

Во избежание дополнительных настроек и изменений при использовании Remote Services убедитесь, что выполняются следующие требования:

- версия микропрограммы панели — 2.19.7 или выше, все панели подключены через Ethernet, интерфейсы Ethernet включены, используются стандартные настройки Ethernet
- службы Remote Connect включены в конфигурации панели FSP-5000-RPS
- Доступен защищенный сетевой шлюз для Remote Services
- имеется компьютер с FSP-5000-RPS версии 5.12.28 или выше и доступом к Интернету

FSE использует SingleKey ID. Дополнительные сведения можно найти на странице SingleKey ID: https://singlekey-id.com

Создание клиента FSE

Если существующий клиент FSE использовать невозможно, необходимо создать его на странице: https://fse.bosch-nexospace.com/login/.

Возможно, вам придется авторизоваться или зарегистрироваться на странице SingleKey ID.

Возможно, вам потребуется принять условия договора и конфиденциальности данных.

FSE отправит вам на указанный адрес электронное письмо со ссылкой для активации.

Вход в существующий клиент FSE

Вы получили приглашение по электронной почте.

1. Перейдите по ссылке активации в электронном письме с приглашением.
2. Выберите клиент, в который необходимо войти. Отобразятся системы этого клиента.

Подключение к FSP-5000-RPS

Для подключения к FSP-5000-RPS потребуется создать маркер доступа.

1. Щелкните свое имя пользователя в FSE и выберите **Create Access Token** (Создать маркер доступа).
2. Запустите FSP-5000-RPS.
3. Щелкните значок параметров и выберите **Options** (Параметры).
4. В окне **Settings** выберите **Remote Services**.
5. В разделе **Account** (Учетная запись) введите свой адрес электронной почты в FSE и пароль FSE, после чего нажмите кнопку **OK**.
6. В окне **Configuration** (Конфигурация) выберите свою систему.
7. В дереве навигации выберите **Remote Services**.
8. Выберите **Remote Portal / Fire System Explorer** в раскрывающемся списке **Access Type** (Тип доступа).
9. Скопируйте созданный маркер доступа:

– в поле **User token** (Маркер пользователя), если вы работаете на личном компьютере,
– или в поле **One time token** во всех остальных случаях.

8.2 Remote Alert

С помощью службы Remote Alert панель отправляет соответствующую информацию о статусе.

Передаваемые данные анализируются с помощью Remote Alert. В случае непредвиденного события пользователь информируется по электронной почте о полученных оповещениях.

Remote Alert также доступна для Private Secure Network.

Частью службы Remote Alert является приложение **Remote Fire Safety**. Приложение позволяет пользователям получать на свои мобильные устройства мгновенные push-уведомления о сигналах тревоги и предупреждениях системы.

Пользователь также может получить доступ к истории уведомлений, которыми можно поделиться по электронной почте или через мессенджер.

Кроме того, приложение предоставляет обновленные сведения о состоянии системы, включая работоспособность, возможность подключения, срок действия лицензии и необходимость обновления микропрограммы пожарной панели.

Приложение можно скачать бесплатно: https://play.google.com/store/apps/details?id=com.bosch.remote_fire_safety&gl=EN или https://apps.apple.com/de/app/remote-fire-safety/id1557422840

8.3 Remote Maintenance

Remote Maintenance позволяет удаленно отслеживать определенные параметры различных элементов системы безопасности, подключенных к пожарной панели. С помощью пользовательского интерфейса можно выполнить пошаговые проверки.

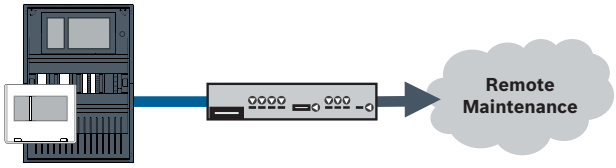


Рис. 8.2: Служба Remote Maintenance

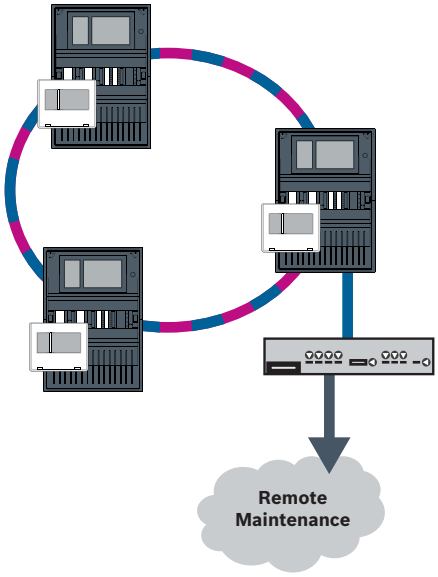


Рис. 8.3: Remote Maintenance

При использовании Remote Maintenance с сетями Ethernet одна панель сети должна быть подключена к маршрутизатору для передачи данных. Все собранные данные передаются из сети с помощью этого подключения.
Remote Maintenance собирает данные о соответствующих LSN-устройствах и функциональных модулях. Полученные данные анализируются и визуализируются для проведения технического обслуживания.

8.4 Remote Maintenance для Private Secure Network

Remote Maintenance можно настроить для сети Private Secure Network: собранные данные будут отправляться в систему центрального сервера управления (CMS).

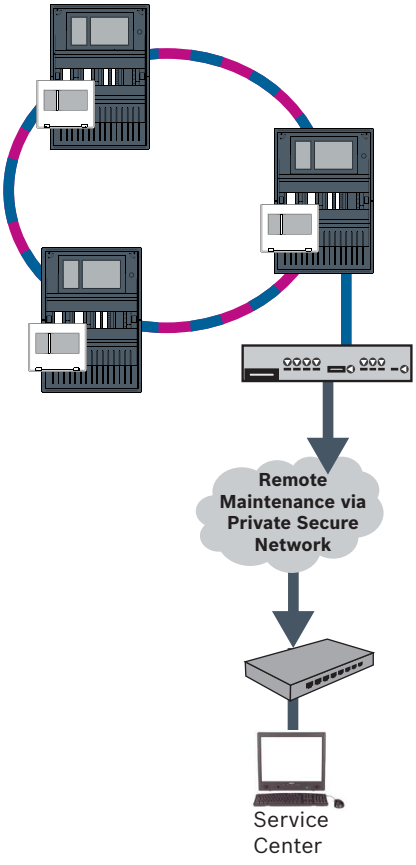


Рис. 8.4: Remote Maintenance для Private Secure Network

Для Remote Maintenance в программе FSP-5000-RPS необходимо ввести IP-адрес сервера и порт системного сервера Remote Maintenance.
Назначьте сети уникальный идентификатор сети панелей.

Коммутатор для подключения CMS необходимо программировать отдельно
Программирование IP-адреса и настроек резервирования коммутатора см. в разделе *Настройка коммутатора, Страница 53*. Поскольку коммутатор установлен в непосредственной близости (без промежуточного пространства), резервирование источника питания не требуется. Поэтому выходы неисправности не используются. Убедитесь в идентичности настроек RSTP в контроллерах панели, FSP-5000-RPS и коммутаторе Ethernet.

9 система управления зданием

Контроллер панели с премиум-лицензией можно подключить к системе управления зданием через интерфейс Ethernet с помощью одного из следующих серверов:

- Сервер FSI: FSI (интерфейс системы пожарной сигнализации) — это собственный протокол связи компании Bosch. Для интеграции с учетом индивидуальных требований предоставляется пакет средств разработки программного обеспечения (SDK).
- Сервер OPC: OPC (OLE для управления процессами) — это стандартизированный протокол связи, соответствующий стандарту Building Integration System (BIS).
- Сервер BACnet: BACnet (сеть управления зданием и автоматизации) — это стандартизированный протокол связи, предназначенный специально для подключения к сторонней системе управления зданием.

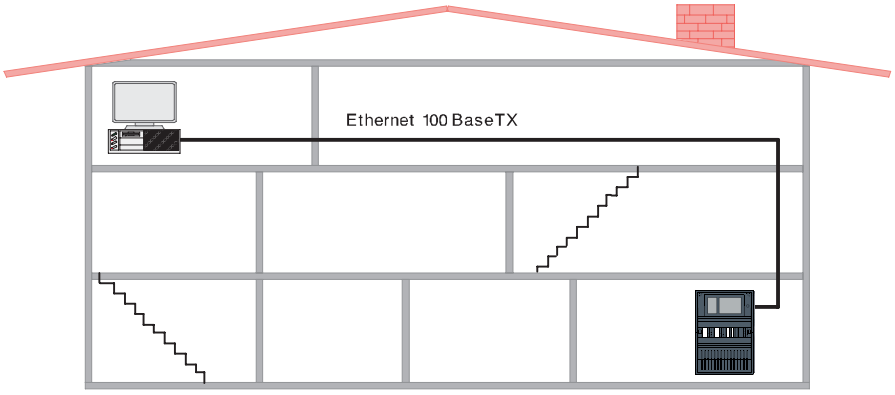


Рис. 9.1: Подключение к системе управления зданием

При подключении к системе управления зданием через Ethernet 100BaseTX в сетях, объединяющих несколько зданий, необходимо узнать у сетевого администратора следующее:

1. Предназначена ли данная сеть для подключений нескольких зданий? (так, не должно быть связанных с техническими средствами помех из-за разницы потенциала земли)
2. Достаточно ли пропускной способности для пользователей данной сети?

Замечание!
При подключении к системе управления зданием соблюдайте инструкции по безопасности, приведенные в разделе *Безопасность, Страница 5*.

Конфигурация в FSP-5000-RPS

Для подключения к системе управления зданием необходимо создать сервер (OPC server, BACnet server, FSI server) в программном обеспечении FSP-5000-RPS.
В программном обеспечении FSP-5000-RPS и на сервере необходимо выполнить следующие настройки: запрограммировать адрес логического узла (**Сетевая группа** и **Сетевой узел**), адрес физического узла (**PNA/RSN**) и параметры IP (**IP-адрес** и **Порт**).
Компания Bosch рекомендует использовать порт 25000 для OPC-сервера и порт 25001 для BACnet server или FSI server.
Необходимо назначить сервер каждой панели или удаленной клавиатуре, с которых требуется передавать статусы. Максимальное количество серверов, которое можно назначить одной панели или удаленной клавиатуре:

- 1 BACnet server
- 2 FSI server
- 1 OPC server
- 2 UGM server

Замечание!
EN 54
Подключение системы управления зданием через интерфейс Ethernet соответствует требованиям стандарта EN 54, только если функции EN 54 выполняются исключительно пожарной панелью. Любые связанное с EN 54 управление или администрирование (например, управление оповещателями или администрирование отключения) системы управления зданием требует индивидуальной EN 54-сертификации всей системы органом сертификации.

Ethernet-коммутатор для подключения системы управления зданием необходимо запрограммировать отдельно

Программирование IP-адреса и настроек резервирования коммутатора Ethernet см. в разделе *Настройка коммутатора, Страница 53*. Поскольку коммутатор установлен в непосредственной близости (без промежуточного пространства), резервирование источника питания не требуется. Поэтому выходы неисправности не используются.
Убедитесь в идентичности настроек RSTP в контроллерах панели, FSP-5000-RPS и коммутаторе Ethernet.

Коммутаторы для подключения системы управления зданием и второго кольцевого шлейфа необходимо запрограммировать отдельно

Программирование IP-адреса и настроек резервирования коммутатора Ethernet см. в разделе *Настройка коммутатора, Страница 53*. В случае этой топологии выходы неисправностей коммутатора должны использоваться только при наличии резервного источника питания для коммутатора. См. раздел *Коммутатор Ethernet, Страница 64*.
Убедитесь в идентичности настроек RSTP в контроллерах панели, FSP-5000-RPS и коммутаторе Ethernet.
Измените RSTP-приоритет для коммутаторов, соединяющих две кольцевых подсети, так как они принадлежат к магистрали.

Сервер необходимо запрограммировать отдельно.

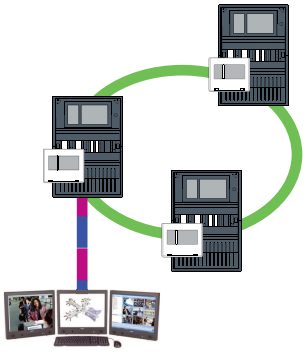
Запрограммируйте адрес логического узла (**Сетевая группа** и **Сетевой узел**), адрес физического узла (**PNA/RSN**) и параметры IP (**IP-адрес** и **Порт**).
Компания Bosch рекомендует использовать порт 25000 для интерфейса Ethernet между пожарной панелью и сервером.
Убедитесь в идентичности настроек ПО конфигурирования FSP-5000-RPS и сервера.

Замечание!

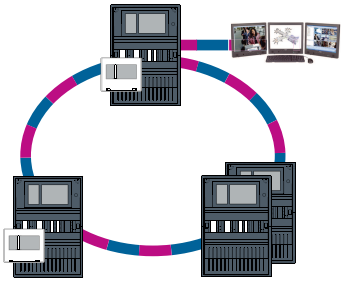
Подробные сведения об установке и настройке сервера BACnet или OPC см. в руководствах по установке и настройке серверов, доступных в онлайн-каталоге на сайте www.boschsecurity.com. Руководство по серверу FSI можно найти в системе extranet (требуются права доступа).

Топологии с системой управления зданием

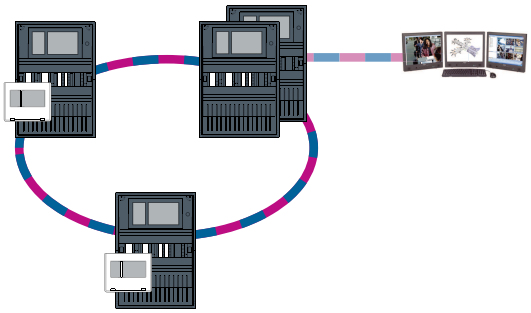
Система управления зданием может быть подключена через кабель Ethernet (медный) или оптоволоконный кабель.



Кольцо CAN с системой управления зданием

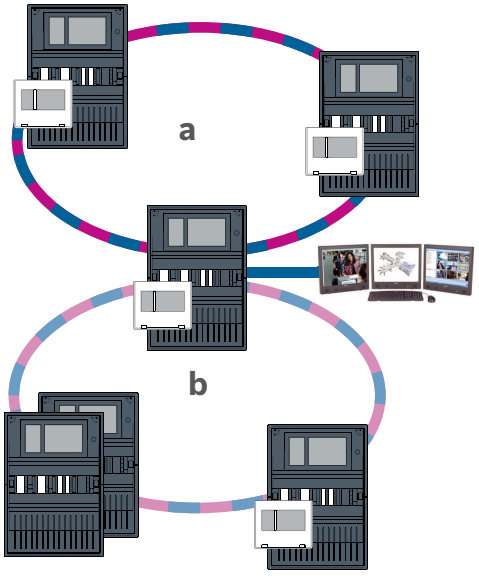


Кольцо Ethernet с системой управления зданием

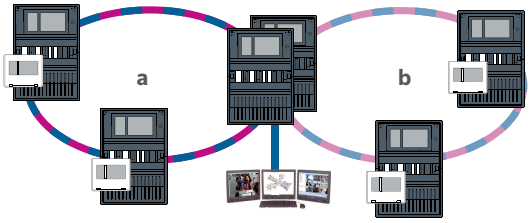


Кольцо Ethernet с системой управления зданием к резервной панели

В следующих топологиях кольцевой шлейф a — магистраль. Кольцевой шлейф b — кольцевая подсеть.



Подключение кольца Ethernet через панель без резервирования



Подключение кольца Ethernet через резервную панель

10 Интеллектуальная передача информации

В этой главе описано техническое решение по защищенному интерфейсу Ethernet между пожарными панелями Bosch и системами речевого оповещения Bosch.
Smart Safety Link — самый надежный и безопасный способ объединения систем пожарной сигнализации и речевого и аварийного оповещения (VAS). Smart Safety Link обеспечивает выдающуюся гибкость и возможность расширения.
Двунаправленная система передачи данных устанавливает контролируемую связь между панелью пожарной сигнализации и системой VAS. При разрыве соединения и пожарная панель, и система VAS выводят сообщение о неисправности. В случае обрыва подключения пользователь может вручную запустить эвакуацию всего здания с помощью вызывной станции системы VAS. Обрыв соединения не приводит к автоматической эвакуации здания. Когда соединение снова установлено, пожарная панель автоматически выполняет повторную синхронизацию текущего состояния

тревоги с системой VAS. В состоянии тревоги пожарная панель может автоматически запускать речевые объявления с помощью виртуальных триггеров системы VAS, которые активируются правилами, настроенными в программном обеспечении FSP-5000-RPS. При запуске эвакуации из системы VAS на пожарной панели отображается контрольное сообщение. В случае неисправности системы VAS в интерфейсе пользователя на пожарной панели появляется сообщение об этом.
Благодаря графическому интерфейсу пользователя AVENAR panel оператор может отключать звук объявлений пожарной панели. Оператор может запросить обзор текущего состояния всех виртуальных триггеров. Каждый виртуальный триггер можно пометить однозначной меткой с информацией о расположении и типе сообщения. Отдельный характерный цвет отражает состояние каждого виртуального триггера. Оператор с правами пользователя L2 может вручную запускать и останавливать голосовые объявления в выбранном виртуальном триггере.
PAVIRO или Praesideo можно подключить к FPA и AVENAR panel.
В связи с сетевой топологией для PRAESENSA требуется интерфейс с шифрованной передачей данных. Используйте только AVENAR panel с микропрограммой контроллера панели версии 4.x для подключения к PRAESENSA.
Smart Safety Link over Ethernet доступна в микропрограмме контроллера панели версии 2.11 и FSP-5000-RPS версии 4.3.

Предупреждение!
Угрозы безопасности в сети Ethernet
Не подключайте PRAESENSA к FPA-5000/FPA-1200 с помощью Smart Safety Link из-за угрозы безопасности в сети Ethernet.

Замечание!
Система речевого и аварийного оповещения, подключенная к панели AVENAR
Каждая пожарная панель, которая физически подключена к системе речевого и аварийного оповещения через Smart Safety Link, требует наличия премиальной лицензии.

Замечание!
Система речевого оповещения, подключенная к FPA
Каждая пожарная панель, физически подключенная к системе речевого оповещения через Smart Safety Link, с микропрограммой версии 3.x не требует лицензионного ключа для речевого оповещения.

10.1 Один прямой интерфейс VAS

Пожарная панель и система речевого и аварийного оповещения могут быть подключены одним кабелем Ethernet TX.

Замечание!
VdS 2540
Система речевого и аварийного оповещения должна быть установлена вплотную к пожарной панели в одном помещении. Иначе требования VdS 2540 для путей передачи данных не будут удовлетворены.

10.1.1 Praesideo и PAVIRO

AVENAR panel и FPA можно напрямую подключить к выделенному порту Ethernet с открытым интерфейсом системного контроллера Praesideo (PRS-NCO-3) или PAVIRO (PVA-4CR12).

Используйте открытый интерфейс для отдельной панели или сети панелей.

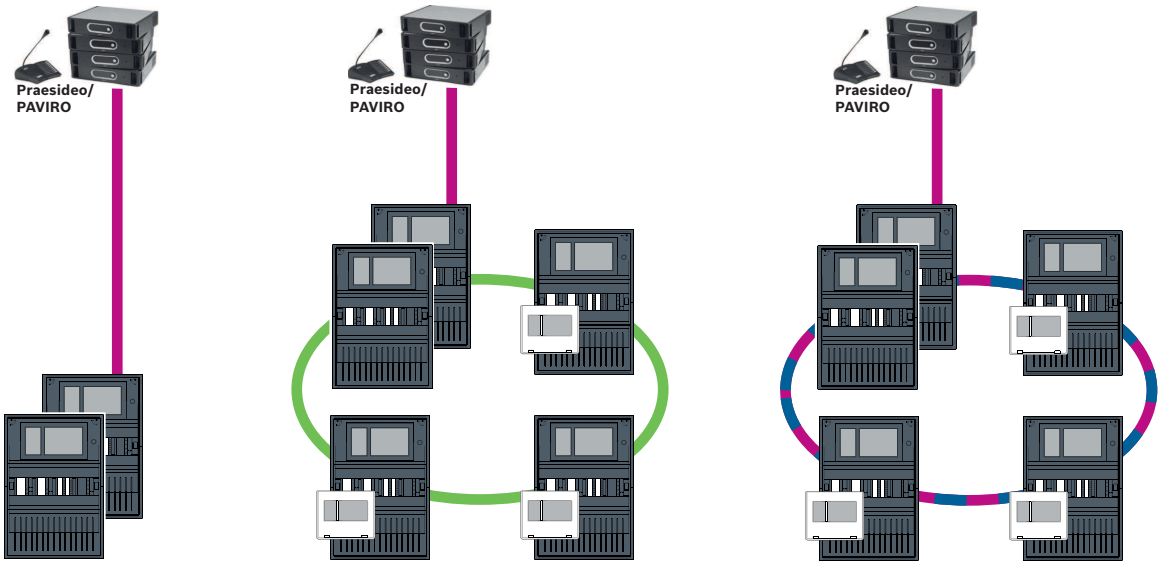


Рис. 10.1: Один прямой интерфейс Praesideo|PAVIRO

Замечание!

Если для прямого подключения к системе Praesideo/PAVIRO будет использоваться контроллер панели MPC-xxxx-B, потребуется соединительный перекрестный кабель, так как ни Praesideo/PAVIRO, ни MPC-xxxx-B не поддерживают функцию Auto-MDI(X).

10.1.2 PRAESENSA

PRAESENSA– это сетевая система речевого и аварийного оповещения, использующая IP-сеть для передачи звука и управления.

Всегда подключайте AVENAR panel через коммутатор Ethernet PRA-ES8P2S, 8xPoE, 2xSFP, к PRAESENSA.

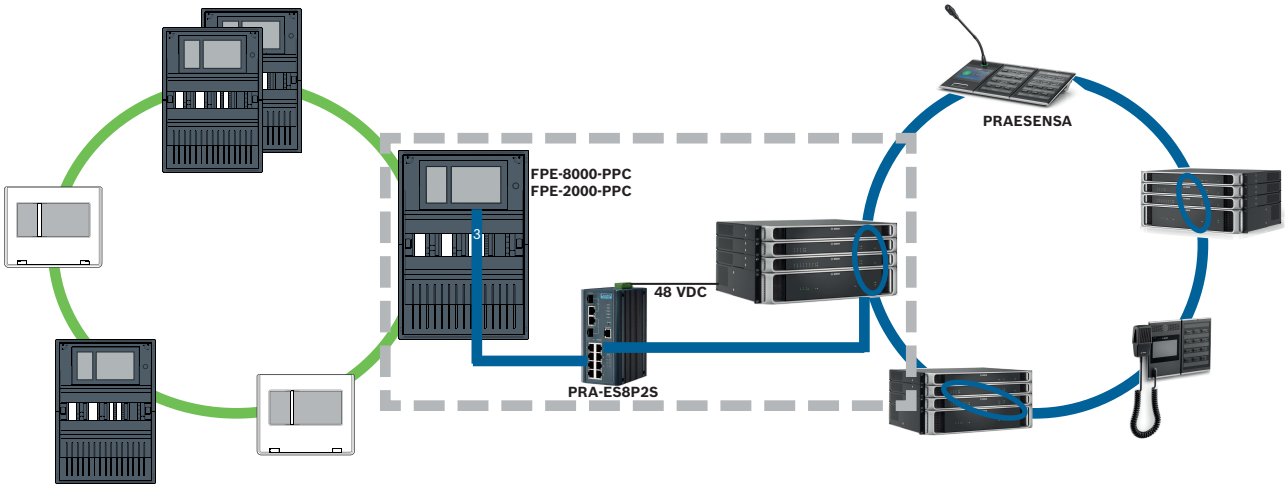


Рис. 10.2: Подключение PRAESENSA к панели AVENAR

Внимание!

Угрозы безопасности в сети Ethernet

Не используйте Smart Safety Link для подключения PRAESENSA к FPA-5000/FPA-1200. Используйте только AVENAR panel и AVENAR keypad 8000 в защищённой сети. Для подключения PRAESENSA к FPA-5000/FPA-1200 используйте контакты реле, как указано в TI2363/2021. Иначе возникают угрозы безопасности в сети Ethernet.

Замечание!

Подключение PRAESENSA к панели AVENAR

— Используйте PRA-ES8P2S только для Smart Safety Link. За исключением системного контроллера PRA-SCL, запрещается подключать оборудование PRAESENSA к портам Ethernet коммутатора Ethernet, 8xPoE, 2xSFP. Не используйте коммутатор Ethernet, 8xPoE, 2xSFP для подключения к системе управления зданием, иерархической панели, шлюзу защищенной сети для служб Remote Services и т. д.

— Используйте панель, содержащую только один контроллер, для подключения к PRAESENSA с помощью Smart Safety Link. Smart Safety Link. Система PRAESENSA еще не совместима с резервным контроллером панели. Панели сети, не подключенные непосредственно к PRAESENSA, могут иметь резервный контроллер панели.

— Используйте топологию шлейфа CAN для сети панелей. Не используйте сеть панелей Ethernet.

— Все AVENAR panel и AVENAR keypad 8000 в сети должны быть оснащены микропрограммой панели 4.x.

Процедура

1. Установите коммутатор Ethernet PRA-ES8P2S в стойку PRAESENSA. Установите PRA-SCL вплотную к AVENAR panel в одном помещении. Не устанавливайте коммутатор Ethernet PRA-ES8P2S в корпусе AVENAR panel.
2. Система PRAESENSA должна обеспечивать питание для PRA-ES8P2S.
3. Настройте коммутатор Ethernet PRA-ES8P2S:
   - разрешите только unicast передачу между FPE-8000-PPC и контроллером PRAESENSA;
   - заблокируйте multicast передачу;
   - отключите RSTP.
4. Проверьте режим PRAESENSA, это должен быть режим DHCP. Режим Zeroconf не поддерживается при использовании Smart Safety Link.
5. Подключите контроллер PRAESENSA одним кабелем Ethernet (RSTP отключен).
6. Для настройки Smart Safety Link панели AVENAR panel выберите **Зашифрованный VAS over IP** в FSP-5000-RPS.

10.2 Несколько прямых интерфейсов VAS

В сети CAN каждую пожарную панель можно подключить к одной системе речевого и аварийного оповещения. Используйте подключение через прямой интерфейс, как указано в *Один прямой интерфейс VAS, Страница 46*.

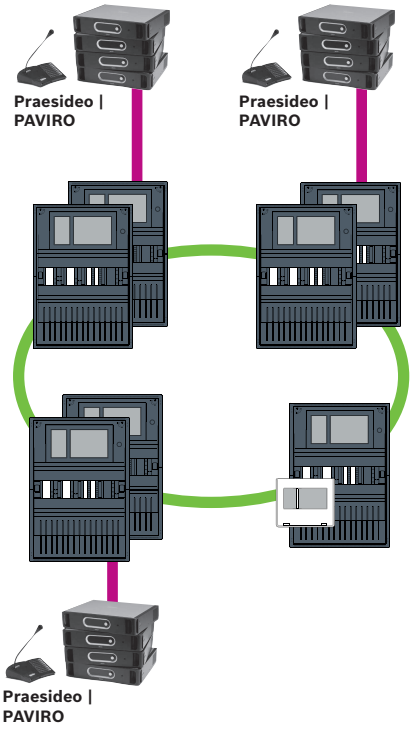


Рис. 10.3: Несколько прямых интерфейсов VAS

Чтобы отключить сетевое подключение панели через IP для каждого узла, выполните указанные ниже действия в FSP-5000-RPS:

1. Выберите узел для отключения панели от сети.
2. Выберите **Использовать параметры Ethernet**.
3. Отмените выбор **Подключение панели через IP**.
4. Нажмите **Применить**.

10.3 VAS, интегрированная в Ethernet сеть панелей

Если Praesideo и PAVIRO интегрированы в сети панелей, система речевого и аварийного оповещения имеет резервный канал связи. Резервный канал связи позволяет устанавливать панель пожарной сигнализации и систему речевого и аварийного оповещения в разных помещениях.

В настоящее время невозможно интегрировать PRAESENSA в Ethernet сеть панелей.

Замечание!

VdS 2540

Система речевого и аварийного оповещения должна быть установлена вплотную к пожарной панели в одном помещении. Иначе требования VdS 2540 для путей передачи данных не будут удовлетворены.

Замечание!

VdS 2540 - Сеть Ethernet

Применительно к Ethernet-сетей панелей следует учитывать, что для установки в Германии, где требуется соответствие стандарту VdS 2540, для всех путей передачи данных должен использоваться оптоволоконный кабель. Единственным исключением является корпус.

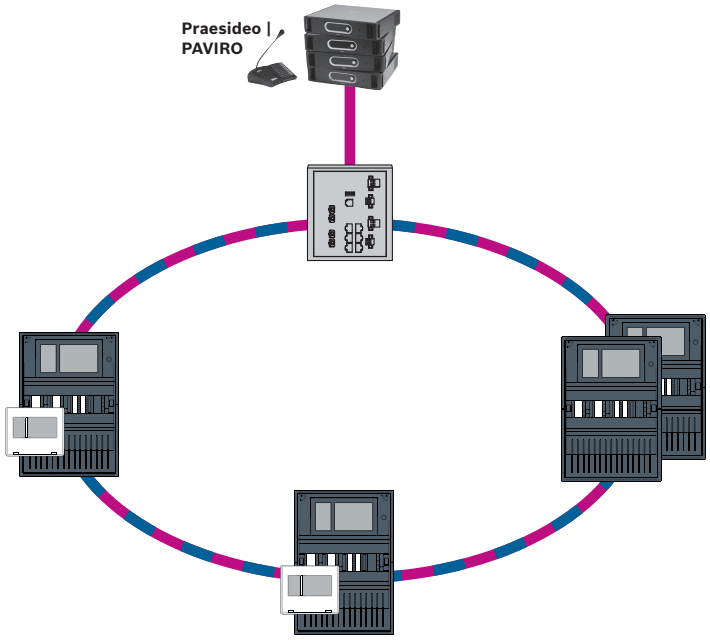


Рис. 10.4: VAS, интегрированная в Ethernet сеть панелей

Чтобы предотвратить передачу относящегося к EN 54-2 многоадресного трафика на маршрутизатор, используйте коммутатор Ethernet (как правило, MM, BPA-ESWEX-RSR20), утвержденный для версии панели 2.8. Активируйте отслеживание IGMP для коммутатора Ethernet, см. соответствующий раздел в главе «Установка» руководства по сетевому подключению.

Система пожарной сигнализации должна обеспечивать питание коммутатора Ethernet.

11 Панель иерархии

Для подключения к иерархической панели необходимо создать сервер UGM server с помощью ПО для конфигурирования FSP-5000-RPS.

В программном обеспечении FSP-5000-RPS и на иерархической панели необходимо выполнить следующие настройки: запрограммировать адрес логического узла (**Сетевая группа** и **Сетевой узел**), адрес физического узла (**PNA/RSN**) и параметры IP (**IP-адрес** и **Порт**).

Компания Bosch рекомендует использовать порт 25001 для интерфейса Ethernet между пожарной панелью и иерархической панелью.

Необходимо назначить сервер каждой панели или удаленной клавиатуре, с которых требуется передавать статусы. Максимальное количество серверов, которое можно назначить одной панели или удаленной клавиатуре:

- 1 BACnet server
- 2 FSI server
- 1 OPC server
- 2 UGM server

Замечание!

Все контроллеры панели и серверы иерархической панели должны находиться в одной подсети и иметь одинаковый адрес многоадресной передачи.

В случае нескольких конфигураций панелей или сетей они должны находиться в одной подсети. Адреса многоадресной передачи должны быть разными.

Чтобы подключить панель к иерархической панели, в FSP-5000-RPS необходимо смоделировать физическую структуру сети. Сюда также входят номера линий между соединяющим контроллером панели и коммутаторами иерархической панели.

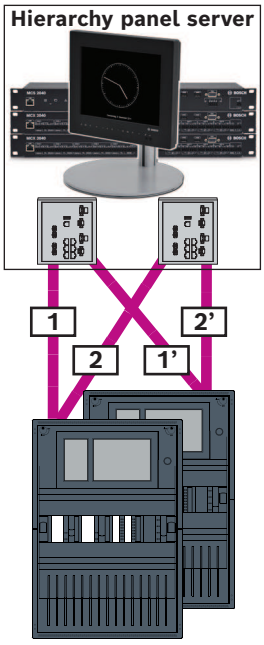


Рис. 11.1: Пример нумерации линий для иерархической панели

12 Установка

Контрольный список

Прежде чем начинать установку сети, убедитесь в выполнении перечисленных ниже условий.

- Ethernet и CAN
  - Необходимые линии кабелей Ethernet TX, Ethernet FX, CAN TX и CAN FX не превышают своей максимальной длины.
  - Запроектированы все периферийные устройства и кабельные разводки для всех панелей.
- Проектирование сети
  - Запланированы и доступны все IP-адреса и сетевые параметры отдельных панелей и дополнительных сетевых компонентов.
  - Доступен обзор устанавливаемых дополнительных компонентов, таких как коммутаторы Ethernet и преобразователи среды, и их кабельного подключения к соседним панелям.
  - Доступен обзор устанавливаемой топологии сети.
  - Запланированы и доступны все параметры резервирования в сети.

12.1 Настройка преобразователя среды

Для использования преобразователя среды необходимо выполнить несколько действий:

- задать DIP-переключатели;
- подключить преобразователь среды к сетевым кабелям FX и CAT5e;
- подать преобразователю среды питание с внутреннего модуля контроллера батареи.

Замечание!
Преобразователи среды питаются только от клеммы источника питания 1.
Поэтому светодиод ошибки на преобразователе среды горит постоянно. Это не влияет на работу устройства.

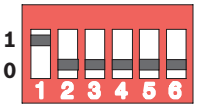
Замечание!
Для организации сетей следует использовать лишь следующие кабели:
Кабель Ethernet
Экранированный Ethernet-кабель CAT5e или выше.
Обратите внимание на минимальные радиусы сгиба, указанные в технических характеристиках кабеля.
Оптоволоконный кабель
Многомодовый: оптоволоконный Ethernet-кабель, дуплекс I-VH2G 50/125µ или дуплекс I-VH2G 62.5/125µ, разъем SC.
Одномодовый: оптоволоконный Ethernet-кабель, дуплекс I-VH2E 9/125µ.
Обратите внимание на минимальные радиусы сгиба, указанные в технических характеристиках кабеля.

Замечание!
Установка преобразователей среды в корпус панели описывается в руководствах по установке монтажных комплектов: FPM 5000 KMC (F.01U.266.845) FPM-5000-KES (F.01U.266.844)

Замечание!
Максимальная секция передачи для многомодовых преобразователей среды через FX: 2000 м.
Максимальная секция передачи для одномодового преобразователя среды через FX: 40 км.

С помощью DIP-переключателей настройте преобразователь среды, как показано на рисунке ниже.

Замечание!
Настройки DIP-переключателей на преобразователях среды можно изменять, только когда они обесточены.



Номер DIP-переключателя	Настройка
1	Функция Link Fault Pass-Through активирована
2	Ethernet: автоматический режим
3	Ethernet: 100 Мбит
4	Ethernet: полный дуплекс
5	Оптоволоконный кабель: полный дуплекс
6	Отключение каналов: выкл.

12.2 Установка Ethernet-коммутатора

Предупреждение!
Лазерный источник света
Не смотрите на источник луча невооруженным глазом или через любые оптические приборы (например, увеличительное стекло, микроскоп). При несоблюдении этого требования возможна потеря зрения при дистанции менее 100 мм. Лазерный свет исходит из видимых контактов или на концах подключенных к ним оптоволоконных кабелей. Используется лазерный диод класса 2M, длина волны 650 нм, выходная мощность < 2 МВт, соответствует IEC 60825-1.

Замечание!
См. Руководство по установке монтажного комплекта коммутатора Ethernet FPM-5000-KES (F.01U.260.523).

12.3 Настройка коммутатора

Чтобы коммутаторы можно было использовать в сети, их необходимо запрограммировать.
Подключите свой портативный компьютер к сети и с помощью программного обеспечения HiDiscovery, предоставляемого производителем, проведите первоначальное программирование коммутаторов. С помощью этого программного обеспечения выполните поиск коммутаторов в сети. Дважды щелкните имя коммутатора, чтобы выбрать его и назначить ему IP-адрес.
После первоначального программирования IP-адреса с помощью веб-браузера можно вызвать пользовательский интерфейс настройки коммутатора.

Замечание!
Точное описание установки и настройки коммутаторов дается в руководстве пользователя производителя. Данные для доступа:
Пользователь: admin
Пароль: private

Пользовательский интерфейс настройки коммутаторов можно вызвать с помощью браузера.
В коммутаторе необходимо выполнить следующие настройки:
- *Назначить IP-адрес, Страница 54*,
- *Задать настройки резервирования, Страница 54*.

Опциональные настройки, например:
- *Настройка реле отказа, Страница 55*,
- *Настройка контроля подключений, Страница 55*,
- *Активация отслеживания IGMP, Страница 56*.

12.3.1 Назначить IP-адрес

Замечание!
Практический совет
В части IP-адресов, соответствующей устройствам, для коммутаторов используйте числа большие 200 (xxx.xxx.xxx.200), если это допускается конфигурацией сети. Это обеспечит более четкое разделение с идентификаторам узла в составе IP-адреса.
Пример
Коммутатор с адресом 192.168.1.201 назначается панели с IP-адресом 192.168.1.1.

Замечание!
Точное описание установки и настройки коммутаторов дается в следующих документах производителя:
Руководство по установке
Справочное руководство по веб-интерфейсу

К пользовательскому интерфейсу настройки коммутаторов можно перейти в браузере.
В меню **Basic Settings (Основные параметры) -> Network (Сеть)** в зависимости от выбранной топологии задайте следующие значения:
- Режим: локальный
- IP-адрес: обязательный IP-адрес, например, 192.168.1.201
- Маска сети: требуемая маска сети, например, 255.255.255.0
- Шлюз: требуемый шлюз, например, 192.168.1.254 или 0.0.0.0, если шлюз не требуется.

Нажмите кнопку **Записать**.

Замечание!
Настройки в отдельных пунктах меню конфигурации коммутатора вступают в силу после нажатия кнопки **Записать**.
Настройки сохраняются только постоянно, то есть они сохраняются даже после перезапуска устройства, если в меню **Основные параметры -> Загрузить/Сохранить** в поле **Сохранить** выбрать пункт **В устройстве** и нажать кнопку **Сохранить**.

12.3.2 Задать настройки резервирования

Так как в сетях панелей FPA в качестве протокола резервирования используется RSTP, этот протокол необходимо активировать и запрограммировать в пользовательском интерфейсе настройки:
В меню **Redundancy (Резервирование) -> Spanning Tree (Связующее дерево) -> Global (Глобальные)** задайте следующие значения:
- Функция: вкл.
- Версия протокола: RSTP
- Конфигурация протокола: те же параметры, что и для контроллеров панели.

Нажмите кнопку **Записать**.

Замечание!
Настройки в отдельных пунктах меню конфигурации устройства switch вступают в силу после нажатия кнопки **Записать**.
Настройки сохраняются только постоянно, то есть они сохраняются даже после перезапуска устройства, если в меню **Основные параметры -> Загрузить/Сохранить** в поле **Сохранить** выбрать пункт **В устройстве** и нажать кнопку **Сохранить**.

12.3.3 Настройка реле отказа

Замечание!
Реле неисправности требуется программировать только для приложений, для которых выполняется хоты бы одно из следующих требований:
Есть соединение между двумя переключателями. Например, это возможно в случае магистрали с подсетями.
Источник питания устройства switch предусматривает резервирование.

Замечание!
Точное описание установки и настройки устройств switch дается в следующих документах производителя:
Руководство по установке
Справочное руководство по веб-интерфейсу

К пользовательскому интерфейсу настройки устройств switch можно перейти с помощью браузера.
В меню **Диагностика -> Контакт сигнала** на вкладке **Контакт сигнала 1** задайте параметру **Режим контакта сигнала** значение **Состояние устройства**.
В меню **Диагностика -> Состояние устройства** в поле **Контроль** задайте следующие значения:
- **Блок питания 1**: **Контролировать**
- **Ошибка подключения**: **Контролировать**

Для всех остальных параметров необходимо задать значение **Игнорировать**.

Замечание!
Параметры раздела **Состояние устройства** также применяются к светодиодному индикатору неисправности устройства switch.

Нажмите кнопку **Записать**.

Замечание!
Настройки в отдельных пунктах меню конфигурации устройства switch вступают в силу после нажатия кнопки **Записать**.
Настройки сохраняются только постоянно, то есть они сохраняются даже после перезапуска устройства, если в меню **Основные параметры -> Загрузить/Сохранить** в поле **Сохранить** выбрать пункт **В устройстве** и нажать кнопку **Сохранить**.

12.3.4 Настройка контроля подключений

Замечание!
Настройка контроля подключений необходима только при использовании реле отказа коммутатора.

Чтобы использовать реле отказа для контроля подключений коммутатора, в конфигурации коммутатора необходимо указать отслеживаемые порты.
Установите флажок **Forward Connection Error (Пересылать ошибку подключения)** для отдельных портов в меню **Basic Settings (Основные параметры) -> Port Configuration (Конфигурация портов)**.

Отслеживаются только те подключения, для которых установлен флажок **Forward Connection Error (Пересылать ошибку подключения)**.
Нажмите кнопку **Записать**.

Замечание!
Настройки в отдельных пунктах меню конфигурации устройства switch вступают в силу после нажатия кнопки **Записать**.
Настройки сохраняются только постоянно, то есть они сохраняются даже после перезапуска устройства, если в меню **Основные параметры -> Загрузить/Сохранить** в поле **Сохранить** выбрать пункт **В устройстве** и нажать кнопку **Сохранить**.

12.3.5 Приоритет QoS

Если коммутаторы используются для обеспечения связи между сетями пожарных панелей и иерархической панелью, в коммутаторах иерархической панели необходимо задать приоритет QoS.
Для иерархической панели UGM-2040 измените в меню QoS/Priorität -> Global настройки поля раскрывающегося списка в Trusted Mode на trustIpDscp.
Нажмите кнопку **Записать**.

Замечание!
Настройки в отдельных пунктах меню конфигурации устройства switch вступают в силу после нажатия кнопки **Записать**.
Настройки сохраняются только постоянно, то есть они сохраняются даже после перезапуска устройства, если в меню **Основные параметры -> Загрузить/Сохранить** в поле **Сохранить** выбрать пункт **В устройстве** и нажать кнопку **Сохранить**.

12.3.6 Активация отслеживания IGMP

Чтобы предотвратить отправку относящегося к EN 54-2 multicast трафика другим системам, подключенным к Ethernet Switch (система речевого и аварийного оповещения интегрирована в сеть панелей Ethernet, Remote Connect), активируйте функцию отслеживания IGMP.
На странице конфигурации IGMP в Ethernet Switch выберите следующий параметры:

1. Включите операцию отслеживания **IGMP**.
2. Активируйте **Запросчик IGMP**.
3. Настройте интервал передачи, с которым RSR20 отправляет пакеты запросов IGMP (например, 4 секунды).
4. Данное время необходимо настроить для участников многоадресной рассылки, которые должны отвечать на запросы IGMP (например, 3 секунды).
5. Выберите **Отказаться** для пакетов с неизвестными адресами многоадресной рассылки.
6. Установите флажок **Отправить для запроса и зарегистрированных портов** для пакетов с известными адресами многоадресной передачи.
7. Включайте IGMP только для портов, к которым подключены другие системы, соединенные с устройством switch. Отключите настройку **Статический порт запросов** для всех портов.

12.4 Сеть CAN

Сетевое подключение и интерфейсы
В контроллере панели есть

– два интерфейса CAN (CAN1/CAN2) для объединения в сеть (кольцевая или радиальная топология)
– два входа (IN1/IN2)
– два интерфейса Ethernet,
– интерфейс USB

В зависимости от типа контроллера панели:

– два дополнительных интерфейса Ethernet
– интерфейс RS232

Обратите внимание, что максимальная длина кабеля для подключения к интерфейсу USBсоставляет 3 м и 2 м — для подключения к RS232.

Адресация и параметры в сети

В зависимости от типа контроллера панели:

– Адрес физического узла задается в микропрограмме панели при ее первом включении
– RSN на механических поворотных переключателях на задней части панели

Для отображения адреса физического узла, если он сохранен в контроллере панели, выполните следующие действия:

▸ Выберите **Конфигурация** -> **Сетевые службы** -> **Ethernet** -> **Использ. настройки Ethernet** -> **Параметры IP** -> **По умолчанию**

Для изменения адреса физического узла, сохраненного в контроллере панели, выполните следующие действия:

▸ Отобразите настройки по умолчанию и измените последний октет **IP-адреса**.

Чтобы изменить механический номер RSN, выполните следующие действия:

▸ На механических поворотных переключателях в задней части панели установите номер RSN и убедитесь, что он отображается на табличке под поворотными переключателями.

Конструкция топологии

Коммутаторы DIP для конфигурации разных топологий находятся сзади.

▸ Пометьте выбранные параметры на табличке рядом с коммутаторами DIP.

Автономная панель и автономная панель с резервированием

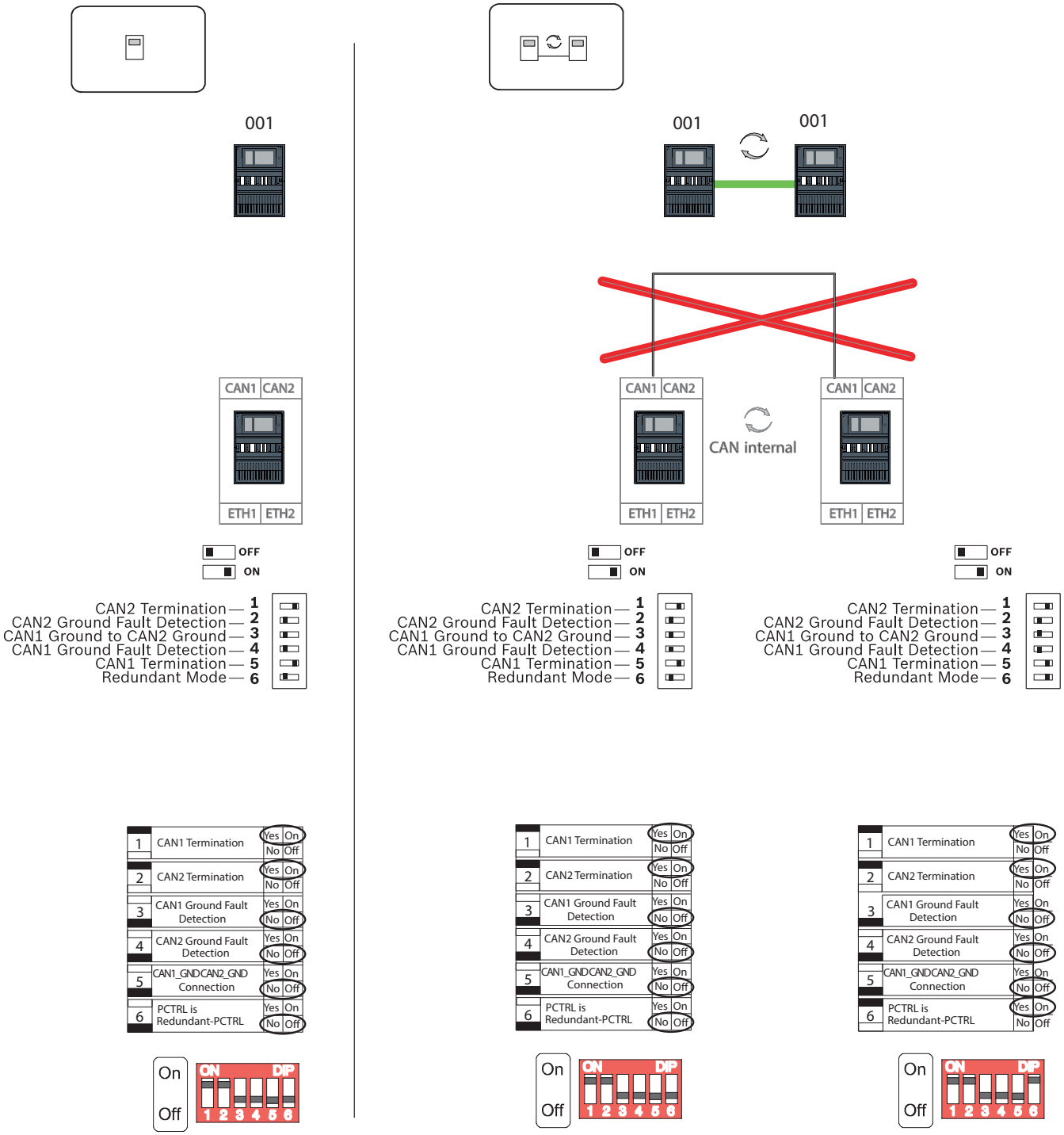


Рис. 12.1: Настройки DIP-переключателя для автономной панели (вверху: AVENAR, внизу: FPA, слева: обычная, справа: с резервированием)

Удаленная клавиатура в качестве резервной панели

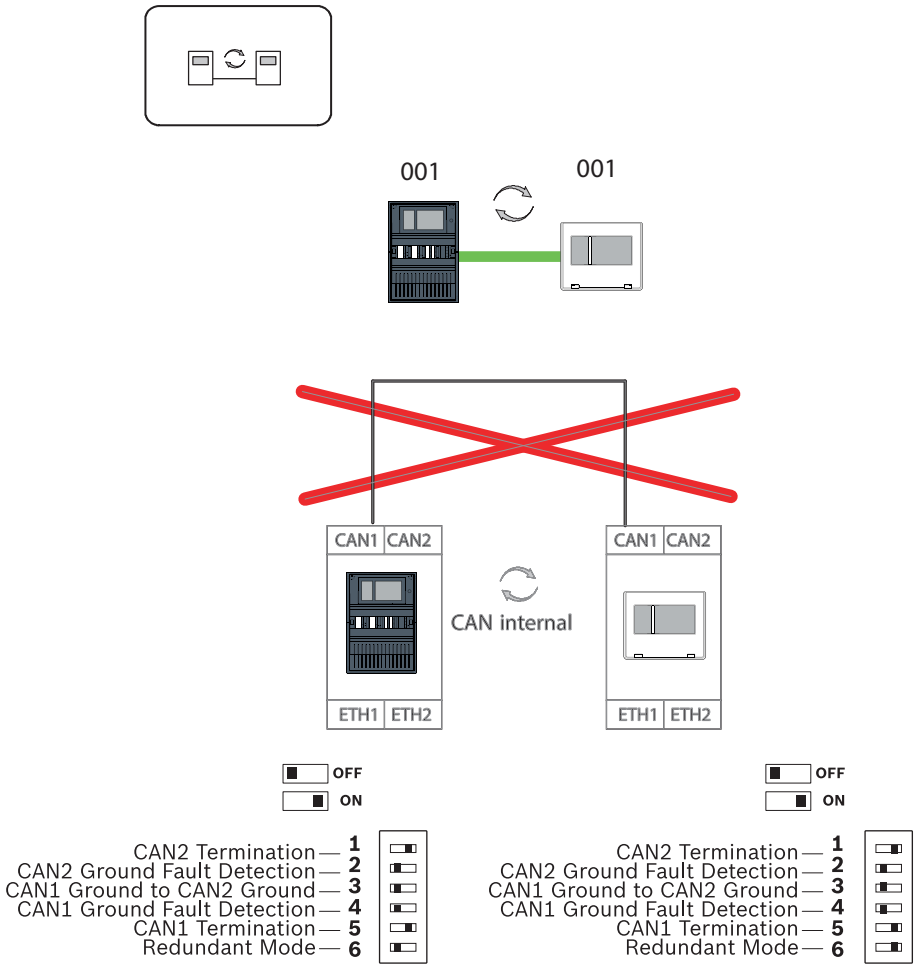


Рис. 12.2: Настройки DIP-переключателя для удаленной клавиатуры в качестве резервной панели (только AVENAR)

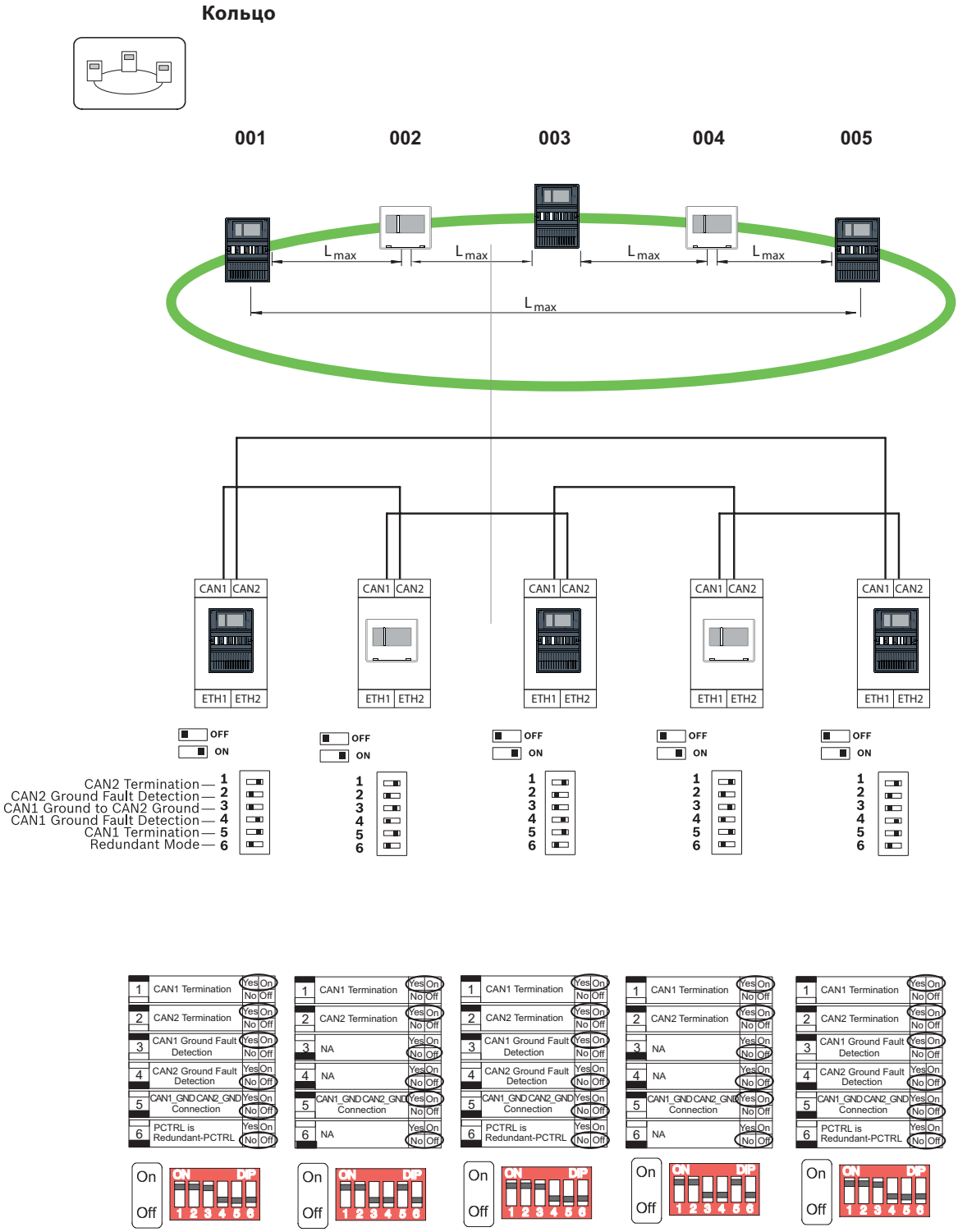


Рис. 12.3: Настройки DIP-переключателей для кольцевой топологии (вверху: AVENAR, внизу: FPA)

Кольцо с резервными панелями

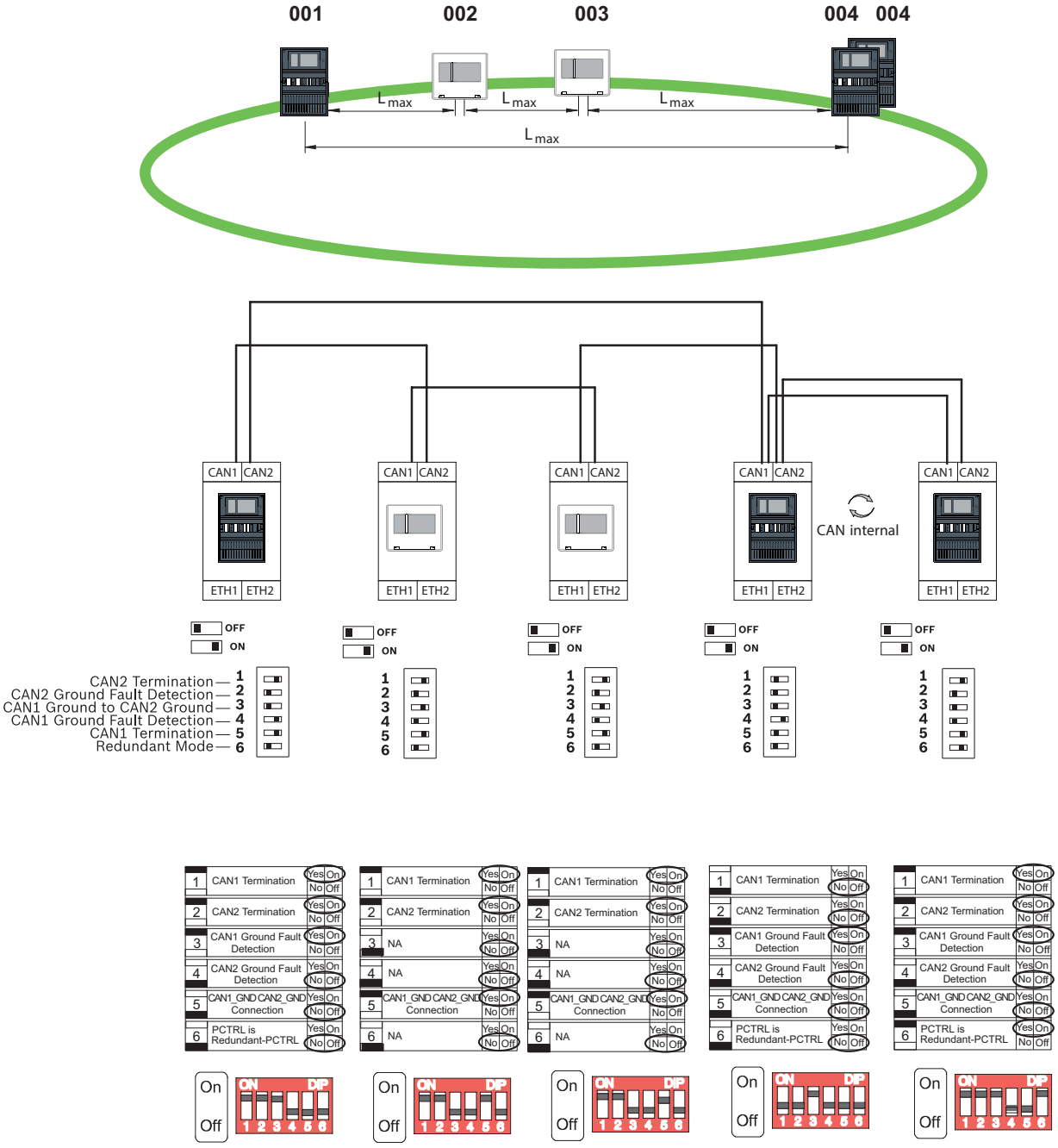


Рис. 12.4: Настройки DIP-переключателей для кольцевой топологии с резервными панелями (вверху: AVENAR, внизу: FPA)

Кольцевая топология с удаленной клавиатурой в качестве резервной панели

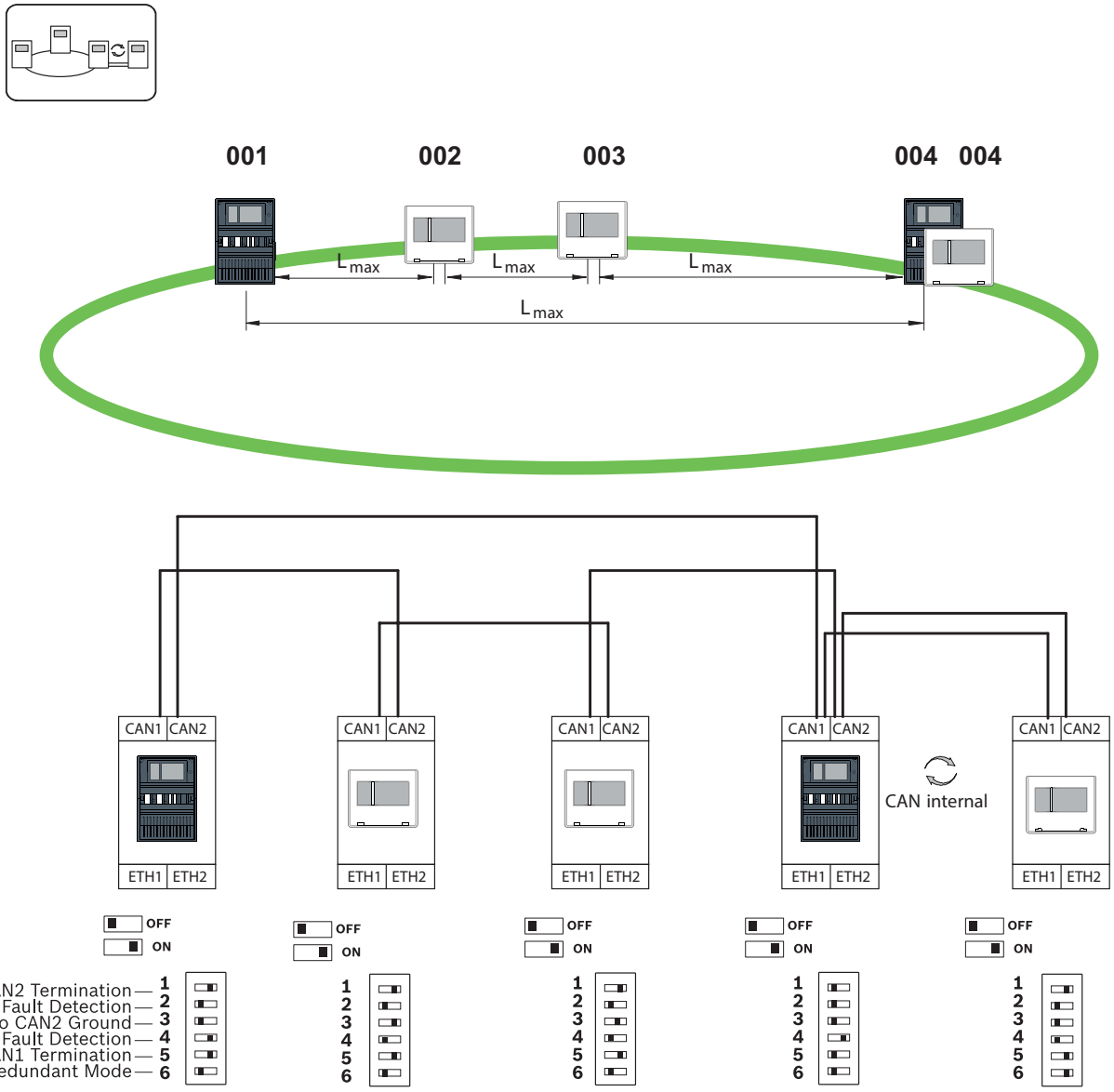


Рис. 12.5: Настройки DIP-переключателя для кольцевой топологии с удаленной клавиатурой (только AVENAR)

13 Кабель Ethernet

Чтобы создать систему, соответствующую стандарту EN 54-2, подключите RSTP-коммутаторы и преобразователи среды к контролируемому источнику питания пожарной панели.

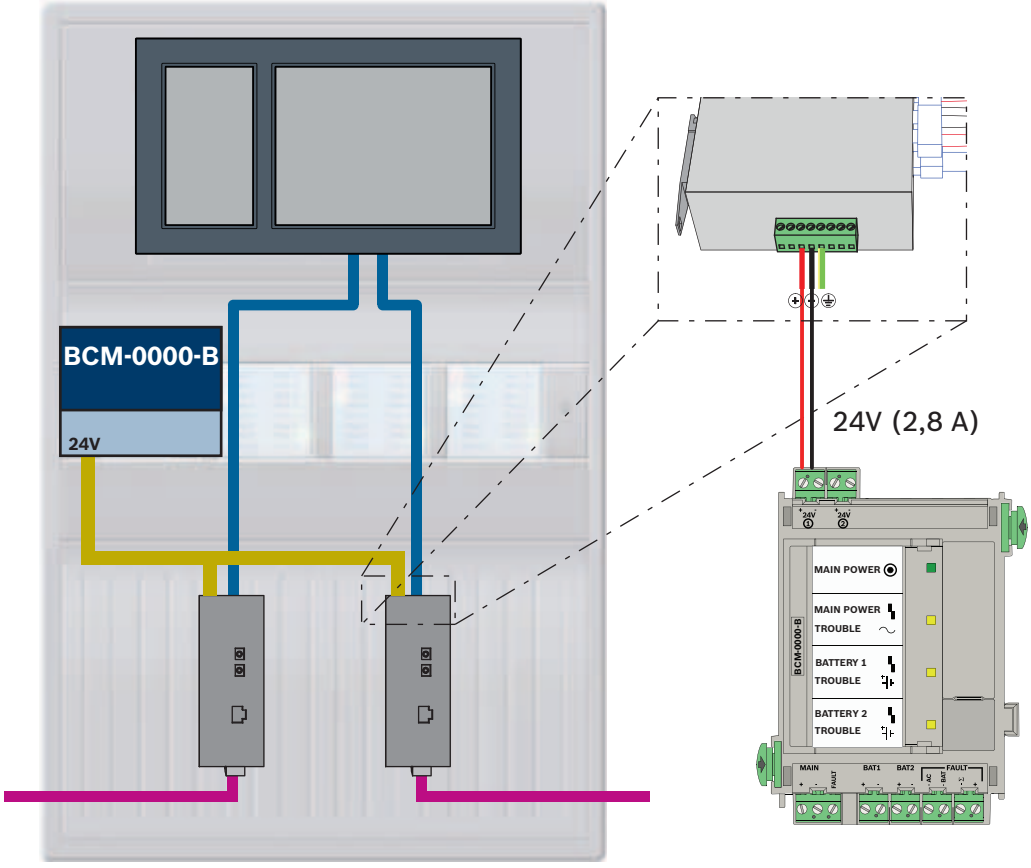
- В качестве источника питания для преобразователей среды и RSTP-коммутаторов используйте выход 24 В модуля контроллера батареи или внешнего источника питания FPP-5000.
- Если вы подключили резервный источник питания или создаете подключение между коммутаторами, необходимо отслеживать выходы неполадок RSTP-коммутатора через входы панели. Например, используйте входы контроллера панели или IOP 0008 A.
- В случае преобразователя среды должна быть активирована функция Link Fault Pass-Through. Конфигурация выполняется с помощью коммутатора DIP или преобразователя среды.

Замечание!
Для организации сетей Ethernet следует использовать только следующие кабели:
Кабель Ethernet
Экранированный Ethernet-кабель CAT5e или выше.
Обратите внимание на минимальные радиусы сгиба, указанные в технических характеристиках на кабель.
Оптоволоконный кабель
Многомодовый: оптоволоконный Ethernet-кабель, дуплекс I-VH2G 50/125µ или дуплекс I-VH2G 62.5/125µ, разъем SC.
Одномодовый: оптоволоконный Ethernet-кабель, дуплекс I-VH2E 9/125µ, разъем SC.
Обратите внимание на минимальные радиусы сгиба, указанные в технических характеристиках на кабель.

13.1 Преобразователь среды

Подключение преобразователей среды

Замечание!
При подключении кабелей FX преобразователей среды отметьте направление передачи по оптоволоконным кабелям.



Значок	Описание
	Кабель Ethernet TX (медный)
	Кабель Ethernet FX (оптоволоконный)

Значок	Описание
	Источник питания
	Передача неисправности
	Медиаконвертер

13.2 Коммутатор Ethernet

Подключение коммутатора

Выходы неисправностей коммутаторов можно подключить к входам контроллера панели или модулю ввода-вывода IOP.

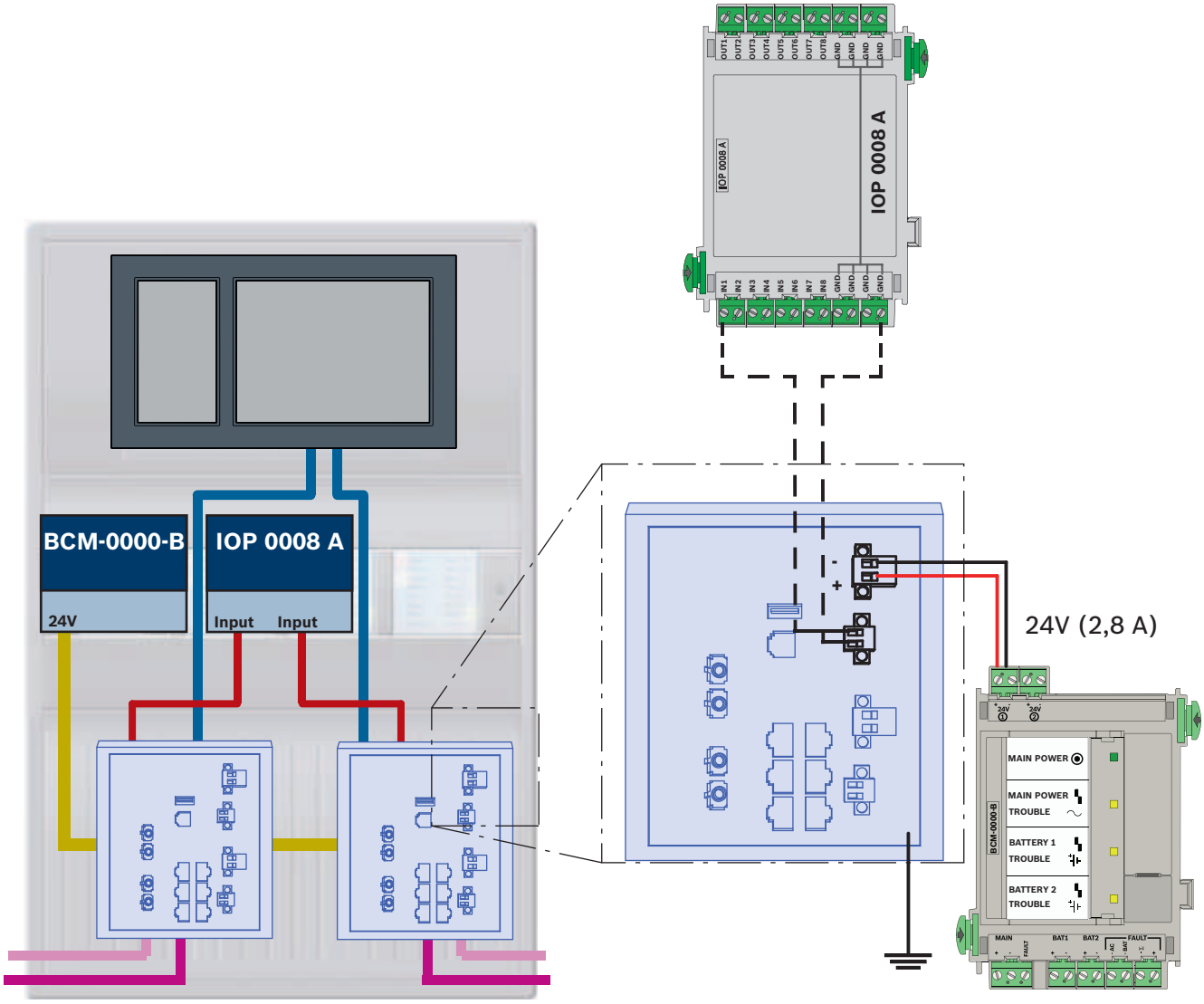
Замечание!

Реле неисправности требуется подключать только для приложений, для которых выполняется хоты бы одно из следующих требований:

Есть соединение между двумя переключателями. Например, это возможно в случае магистрали с подсетями.

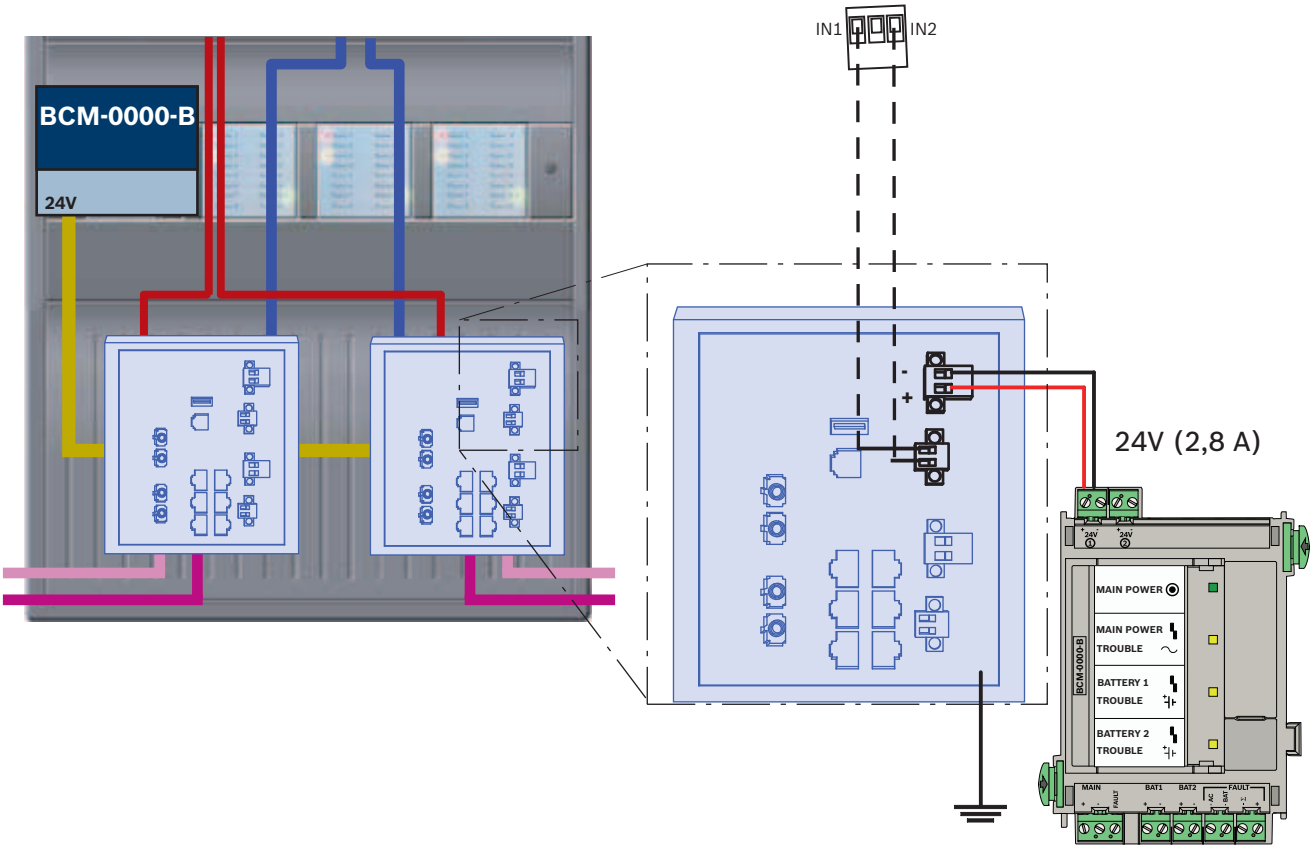
Источник питания переключателя предусматривает резервирование.

Подключение коммутаторов с реле неисправности к входам модуля IOP:



Значок	Описание
	Кабель Ethernet TX (медный)
	Кабель Ethernet FX (оптоволоконный)
	Источник питания
	Передача неисправности
	RSTP-коммутатор

Подключение коммутаторов с реле неисправности к входам контроллера панели



Значок	Описание
	Кабель Ethernet TX (медный)
	Кабель Ethernet FX (оптоволоконный)
	Источник питания
	Передача неисправности
	RSTP-коммутатор

Замечание!
Для подключения коммутаторов нельзя использовать сетевой кабель из комплекта. Используйте экранированный Ethernet-кабель CAT5e или выше.

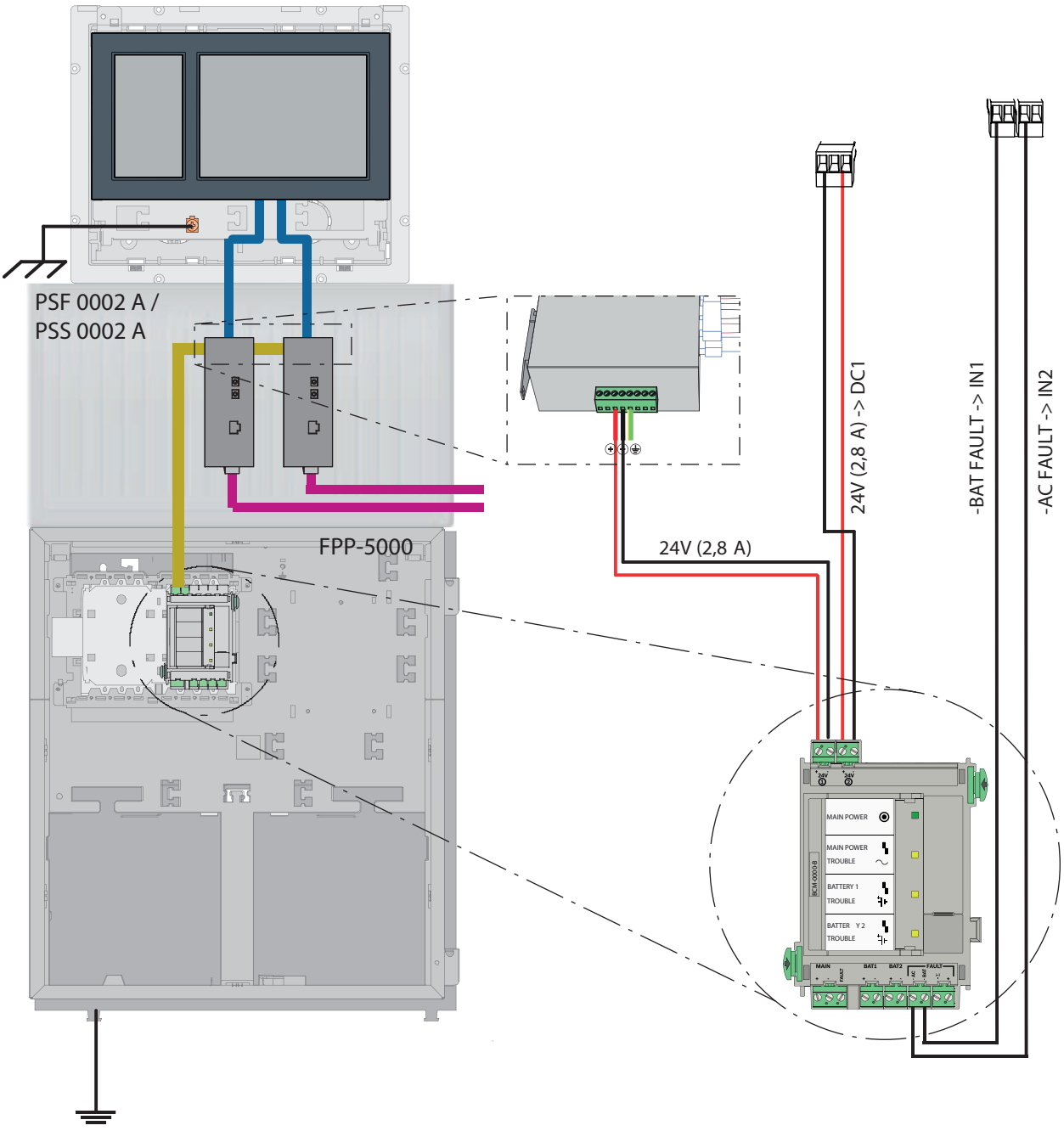
13.3 Удаленная клавиатура

Внимание!
Рабочее заземление удаленной клавиатуры всегда должно быть в рабочем положении при подключении к сети панелей Ethernet.

Замечание!
Для подключения удаленной клавиатуры к сети панелей Ethernet используйте только медиаконвертеры.
Для удаленной клавиатуры не допускается использование коммутаторов.

Подключение к удаленной клавиатуре (в соответствии со стандартом VdS 2540)
В следующем примере для питания удаленной клавиатуры используется внешний источник питания FPP-5000. Подключение к сети устанавливается через 2 медиаконвертера в PSS 0002 A или USF 0000 A.

Замечание!
Внешний источник питания FPP-5000 и дополнительный корпус для медиаконвертеров должны быть установлены вплотную с удаленной клавиатурой. Провода питания удаленной клавиатуры и медиаконвертера не контролируются на предмет короткого замыкания или обрыва на начальной стадии, поэтому они должны быть установлены в корпусах, которые монтируются вплотную к корпусу удаленной клавиатуры.



Значок	Описание
	Кабель Ethernet TX (медный)
	Кабель Ethernet FX (оптоволоконный)
	Источник питания
	Медиаконвертер

14 Параметры FSP-5000-RPS

Программа конфигурирования RPS позволяет запрограммировать всю сеть через USB-порт, сетевой интерфейс или последовательный интерфейс панели. Для этого на панелях необходимо настроить сетевые параметры и перезапустить их, чтобы ввести сеть в эксплуатацию.
Также можно воспользоваться сетевым интерфейсом устройства switch, подключенного к данной сети.

14.1 Сетевые узлы

В программе настройки FSP-5000-RPS необходимо запрограммировать все сетевые узлы и загрузить эту конфигурацию в сеть. Для этого выполните указанные ниже действия.

- Подключите узлы FPA.
  - Установите физический адрес узла (**PNA/RSN**) на каждом узле
- Задайте номера линий для сегментов сети, чтобы создать запланированную топологию.
- Проверьте отображение топологии, чтобы убедиться в ее правильности.
- При необходимости подключите систему управления зданием, систему голосового оповещения, иерархическую панель и коммутаторы
- Отредактируйте параметры Ethernet и IP.
  - Назначьте IP-адреса или примите стандартные настройки, если в топологии меньше 20 RSTP-коммутаторов
  - Выберите протокол резервирования, соответствующий заданной топологии.
- Выполните проверку соответствия.
- Подключитесь к сети через Ethernet, USB или последовательный интерфейс.
- Выполните множественный вход в систему.
- Выполните полное автоопределение для каждой панели.
- Запросите сведения о конфигурации и завершите все задачи.

После перезапуска сети проверьте сообщения об ошибках и при необходимости исправьте их.

14.2 Номера линий

Каждому соединению в используемой сети необходимо назначить номер линии. Не имеет значения, какое это соединение: CAN или Ethernet.
Один номер линии можно использовать как для CAN-соединений, так и для Ethernet-соединений. Однако для удобства работы с сетевыми подключениями следует использовать разные диапазоны номеров.
Обратите внимание, что при использовании **Сеть** как **Тип линии** в окне **Сетевой интерфейс** необходимо задать номер 0 для всех подключений.

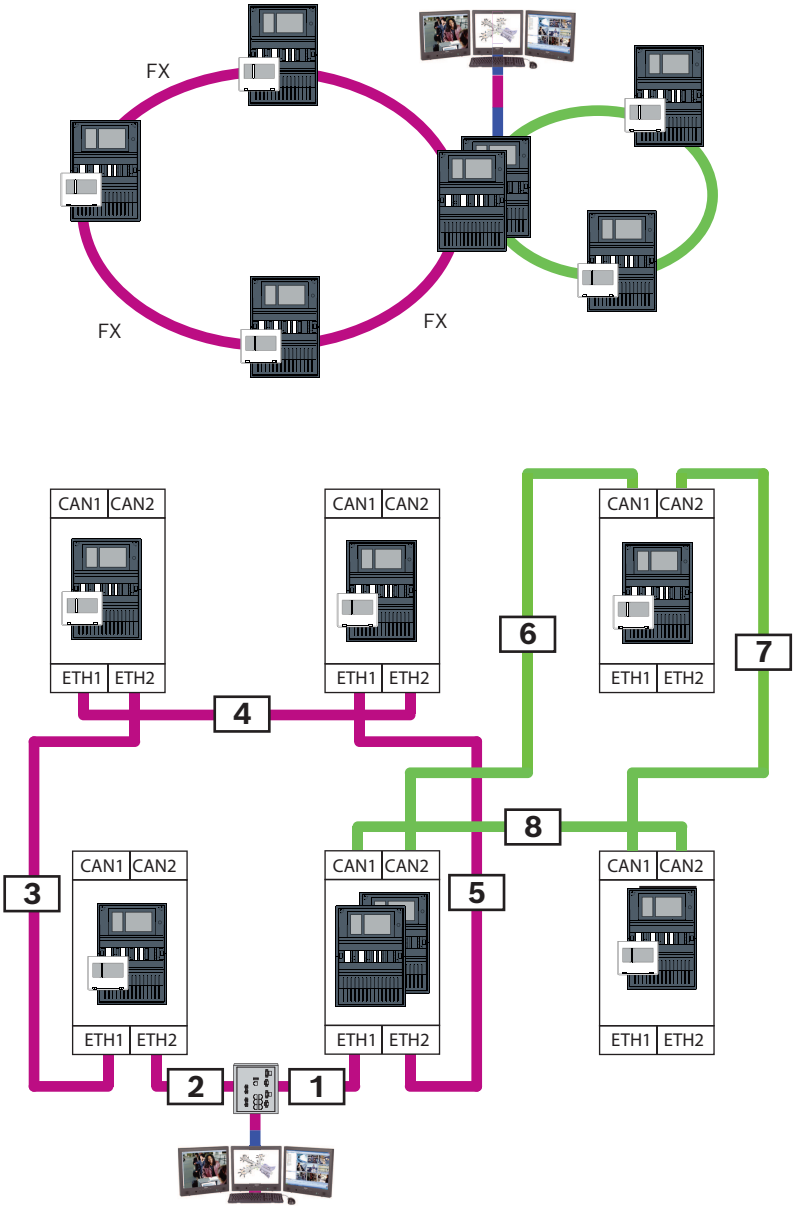


Рис. 14.1: Пример сети и возможной нумерации линий

14.3 Коммутаторы

Если в сети используются устройства switch, такие устройства switch следует создать в программе настройки FSP-5000-RPS. Каждому созданному устройству switch можно назначить до 128 портов. Чтобы создать сеть, отдельным портам можно назначить номера подключенных линий.

15 Приложение

15.1 Сообщения об ошибках Ethernet

Обратите внимание, что в каждом случае ошибки отображаются сообщение об ошибке и групповая ошибка.

Физ. адрес	Логич. адрес	Сообщение об ошибке	Описание и возможная причина
Групповые ошибки связанные с общей неисправностью сети			
135.0.1.0	Сеть 1.0	**Общая неисправность сети**	Имеется несовместимая версия ПО сети панелей. Существует 2 разные версии программного обеспечения.
Групповые ошибки, связанные с сетью			
135.0.6.1	Сеть 2.1	**Дублировать IP-адрес**	IP-адрес назначен дважды.
135.0.6.2	Сеть 2.2	**Параметры IP**	Конфигурация IP указанной в отчете панели отличается от конфигурации RPS
135.0.6.3	Сеть 2.3	**Настройки резервирования**	Настройка резервирования (RSTP, параметр RSTP, двойное подключение или ничего) указанной в отчете панели отличается от конфигурации RPS.
Групповые ошибки, связанные с протоколом RSTP (Rapid Spanning Tree Protocol)			
135.0.7.1	Сеть 3.1	**RSTP Переход на аварийный режим**	Указанная в отчете панель переведена из режима RSTP в режим STP (режим совместимости). К данной сети подключено STP-устройство.
135.0.7.2	Сеть 3.2	**RSTP Изменение топологии**	Изменилась топология сети RSTP. Например, в сеть добавлено другое RSTP-устройство. Это сообщение также может появляться в случае прерывания в линии.
135.0.7.3	Сеть 3.3	**RSTP Тип канала точка-точка**	RSTP-порт указанной в отчете панели не находится в состоянии точка-точка. Например, к RSTP-порту было подключено несколько RSTP-устройств. Или к RSTP-порту было подключено еще одно RSTP-устройство посредством полудуплексной линии.
Групповые ошибки, связанные с сетевым подключением			
135.0.5.1	Сетевое подключение 1.0	**Неисправность CAN 1**	Передача данных в шину CAN 1 ограничена. Возможные причины включают: разрыв кабеля, кабель не подключен, помехи в кабеле.
135.0.5.2	Сетевое соединение 2.0	**Неисправность CAN 2**	Передача данных в шину CAN 2 ограничена. Возможные причины включают: разрыв кабеля, кабель не подключен, помехи в кабеле.
135.0.5.3	Сетевое соединение 3.0	**Неисправность Ethernet 1**	Передача данных в линию Ethernet 1 ограничена. Возможные причины включают: разрыв кабеля, кабель не подключен, помехи в кабеле.
135.0.5.4	Сетевое соединение 4.0	**Неисправность Ethernet 2**	Передача данных в линию Ethernet 2 ограничена. Возможные причины включают: разрыв кабеля, кабель не подключен, помехи в кабеле.

Указатель

Символы

E

L

M

P

R

Bosch Sicherheitssysteme GmbH
Robert-Bosch-Platz 1
70839 г. Герлинген
Германия
www.boschsecurity.com

Решения в сфере управления зданиями для улучшения качества жизни

202503251638