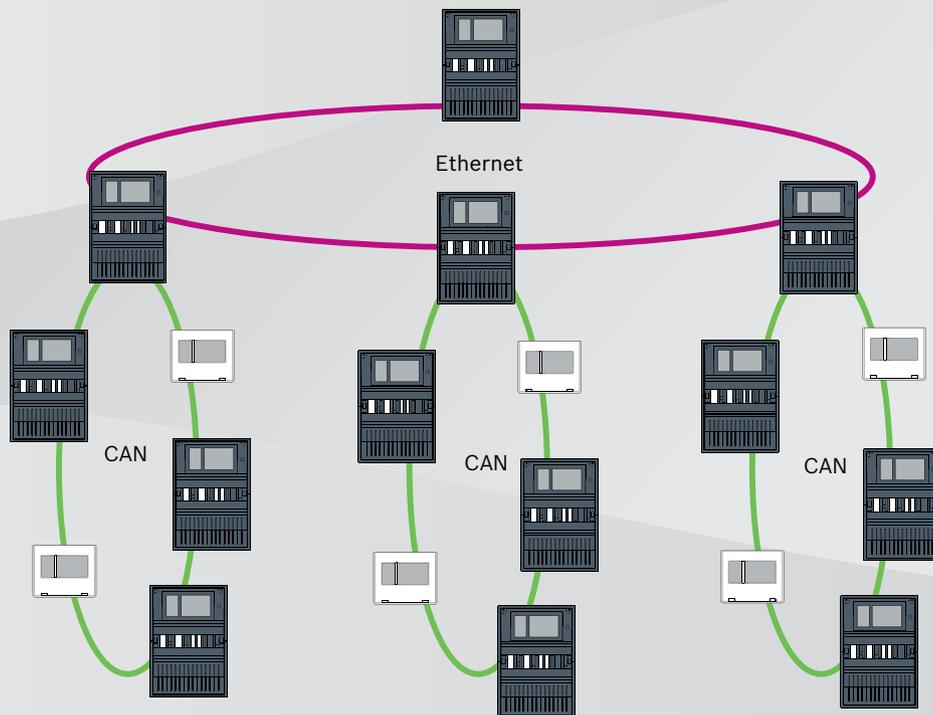




**BOSCH**

## AVENAR panel серии | FPA-5000 | FPA-1200



ru

Networking manual



# Содержание

<b>1</b>	<b>Безопасность</b>	<b>5</b>
1.1	Организационные меры для ПК, на которых выполняются клиенты служб	5
1.2	Пояснение символов безопасности	6
1.3	Примечания по безопасности	6
<b>2</b>	<b>Введение</b>	<b>8</b>
<b>3</b>	<b>Обзор системы</b>	<b>8</b>
<b>4</b>	<b>Топологии</b>	<b>11</b>
4.1	Кольцо CAN	16
4.2	Кольцо Ethernet	16
4.3	Кольцо Ethernet с OPC-сервером	16
4.4	Кольцо Ethernet с OPC-сервером к резервной панели	17
4.5	Двойное кольцо Ethernet/CAN	17
4.6	Кольцо CAN с сегментами Ethernet	17
4.7	Магистраль Ethernet с кольцевыми подсетями (Ethernet/CAN)	18
4.8	Подключение колец Ethernet	20
<b>5</b>	<b>Сеть Ethernet</b>	<b>21</b>
5.1	Протоколы	22
5.2	Диаметр сети	22
5.3	Используемые кабели	24
5.4	Создание или изменение сети Ethernet	25
<b>6</b>	<b>Сеть CAN</b>	<b>26</b>
6.1	Создание или изменение сети CAN	28
<b>7</b>	<b>Схема сетевого подключения Ethernet и CAN</b>	<b>28</b>
7.1	Ethernet-сеть панелей	30
7.2	CAN-сеть панелей	30
7.3	Подключение служб к панели	31
7.4	Ethernet-сеть панелей с резервными панелями	32
7.5	CAN-сеть панелей с резервными панелями	32
7.6	Сеть панелей с двумя кольцами Ethernet	33
7.7	Сеть панелей с двумя кольцами Ethernet и резервными панелями	33
7.8	Подключение Ethernet- и CAN-среды с резервными панелями	34
7.9	Подключение удаленных служб к резервным панелям	34
<b>8</b>	<b>Службы Remote Services</b>	<b>35</b>
8.1	Служба Remote Connect	35
8.2	Remote Alert	37
8.3	Remote Maintenance	38
8.4	Remote Portal	40
<b>9</b>	<b>Системы речевого и аварийного оповещения</b>	<b>42</b>
<b>10</b>	<b>Установка</b>	<b>44</b>
10.1	Настройка преобразователя среды	44
10.2	Установка Ethernet-коммутатора	45
10.3	Настройка коммутатора	45
10.3.1	Назначить IP-адрес	46
10.3.2	Задать настройки резервирования	47
10.3.3	Настройка реле отказа	47
10.3.4	Настройка контроля подключений	48
10.3.5	Приоритет QoS, только для UGM-2040	48
10.3.6	Активация отслеживания IGMP	48

---

<b>10.4</b>	Сеть CAN	<b>49</b>
<b>11</b>	<b>Кабельная сеть</b>	<b>54</b>
<b>11.1</b>	Преобразователь среды	<b>55</b>
<b>11.2</b>	Коммутатор Ethernet	<b>56</b>
<b>11.3</b>	Удаленная клавиатура	<b>59</b>
<b>12</b>	<b>Параметры FSP-5000-RPS</b>	<b>61</b>
<b>12.1</b>	Сетевые узлы	<b>61</b>
<b>12.2</b>	Номера линий	<b>61</b>
<b>12.3</b>	Коммутаторы	<b>62</b>
<b>12.4</b>	ОПС-серверы	<b>62</b>
<b>12.5</b>	Серверы UGM-2040	<b>63</b>
<b>13</b>	<b>Приложение</b>	<b>64</b>
<b>13.1</b>	Сообщения об ошибках Ethernet	<b>64</b>
	<b>Указатель</b>	<b>66</b>

---

# 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!**

Указывает на опасную ситуацию, которую если не избежать, может привести к травмам малой или средней тяжести.



#### **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

#### Преобразователь среды



#### **Предупреждение!**

Лазерный источник света

Не смотрите на источник луча невооруженным глазом или через любые оптические приборы (например, увеличительное стекло, микроскоп). Невыполнение этого требования опасно для глаз при расстояниях менее 100 мм. Свет выходит из зрительных терминалов и на концах подключенных к ним оптоволоконных кабелей. Лазерный диод класса 2M, длина волны 650 нм, выходная мощность < 2 МВт, соответствует IEC 60825-1.

## Службы 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.



### Замечание!

Для построения централизованной сети пожарной сигнализации необходима выделенная сеть Ethernet.

Использование системы автоматического пожаротушения в любой другой сети Ethernet возможно исключительно на собственный рынок 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.

## 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

В соответствии с требованиями VdS 2540 использовать в качестве путей передачи данных следует оптоволоконный кабель для подключений Ethernet. Для подключений внутри корпуса можно использовать кабели Ethernet TX.



### 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.

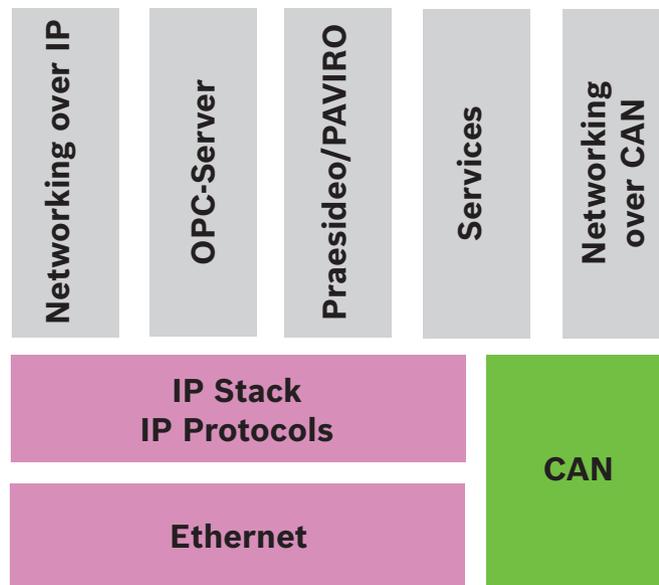
Монтаж отдельных компонентов подробно описывается в соответствующих руководствах по установке.

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

- Связь по TCP/IP

В FSP-5000-RPS в настройках сети Ethernet разрешите связь между панелями.

- Серверы OPC  
Добавьте OPC-сервер в конфигурацию FSP-5000-RPS.
- Подключение Praesideo/PAVIRO  
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!**



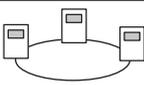
**Непреднамеренная передача данных**

Если интерфейс Ethernet контроллера панели используется только для связи с OPC-сервером 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.

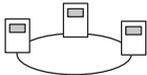
Для работы со службами на основе Ethernet или TCP/IP необходимо включить интерфейсы Ethernet и задать правильные параметры TCP/IP.

**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-	Резервный контроллер панели может иметь стандартную	Невозможно	Невозможно

Топология	AVENAR panel 8000, премиум-лицензия	AVENAR panel 8000, стандартная лицензия.	AVENAR panel 2000, премиум-лицензия	AVENAR panel 2000, стандартная лицензия.
	лицензию. В качестве резервного контроллера панели также можно использовать удаленную клавиатуру.	лицензию. В качестве резервного контроллера панели также можно использовать удаленную клавиатуру.		

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!**

Резервный контроллер панели

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



## 4 Топологии

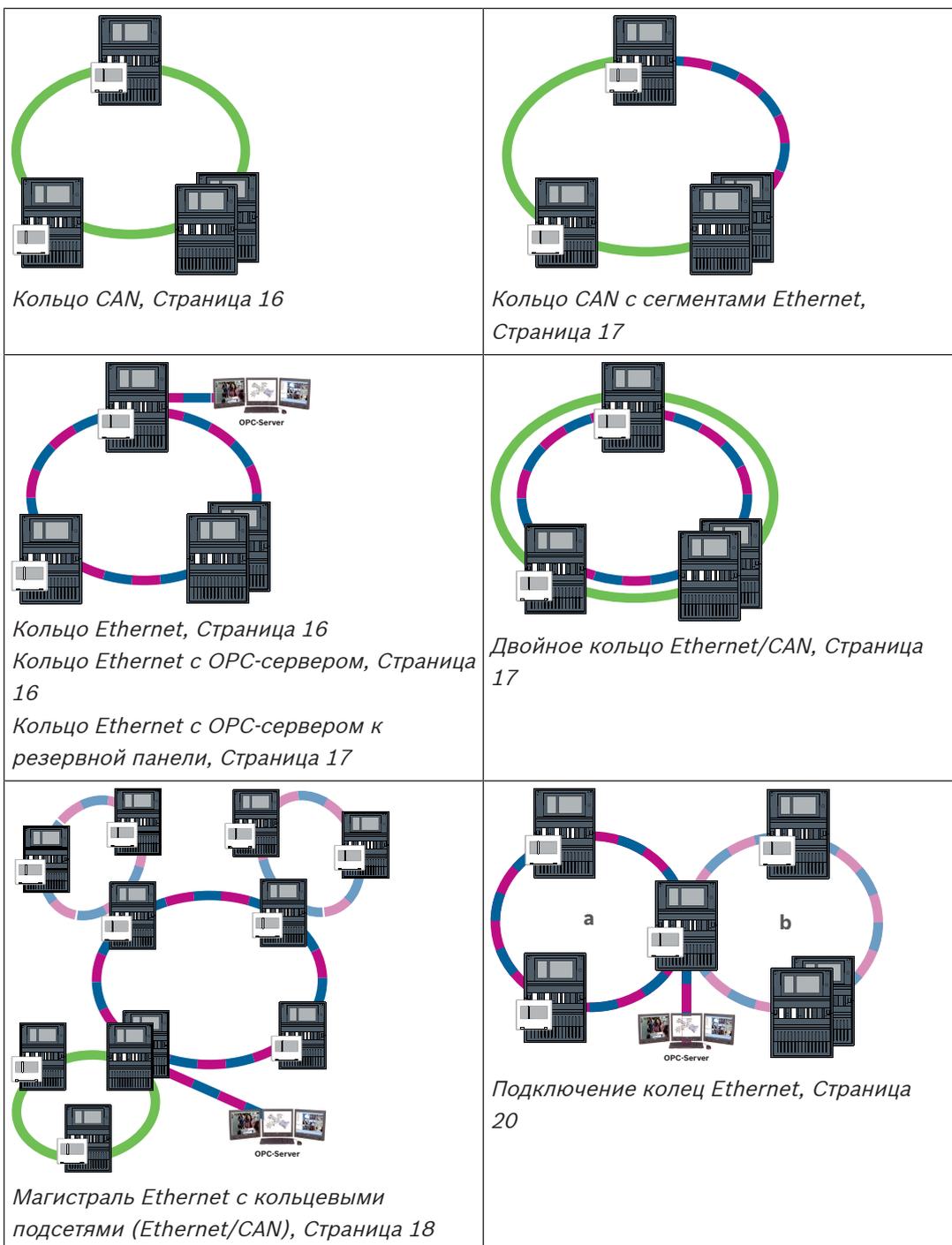
В этом документе описываются различные сетевые топологии систем пожарной сигнализации. Топологии описываются независимо от типа пожарных панелей.



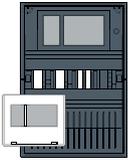
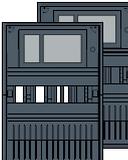
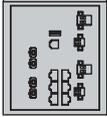
### Замечание!

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.



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)
	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)
	Медиаконвертер
	Защищенный сетевой шлюз для Remote Services

### Ограничения в сети

Число панелей и удаленных клавиатур, которые можно подключить к сети, зависит от выбора сетевой топологии.

Подключенные к сети панели и удаленные клавиатуры называются узлами.

- Максимальное число точек обнаружения в сети: 32768.
- Максимальное число точек обнаружения для каждой подключенной к сети панели: 2048.
- Число узлов в каждой системе зависит от типа топологии.  
Узел — это либо контроллер панели, либо удаленная клавиатура.
- Максимальное число узлов в кольцевой топологии: 32.
- При использовании одной панели FSP-5000-RPS можно назначить до 3 настроенных удаленных клавиатур.

Проводка кабелей между узлами и его максимально допустимая длина также определяется выбором топологии.

В одну сеть можно объединить до 32 контроллеров панели, удаленных клавиатур и OPC-серверов.

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 или удаленная клавиатура 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 точек обнаружения. 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 точек обнаружения, необходимо спроектировать панель с резервированием. RSTP-коммутатор, подключающий 2 кольца, обеспечивает резервирование.

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



#### 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 22*.

- 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.

#### Подключение к BIS с помощью OPC-сервера

При подключении к системе управления зданием (BIS) через OPC-сервер и 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?

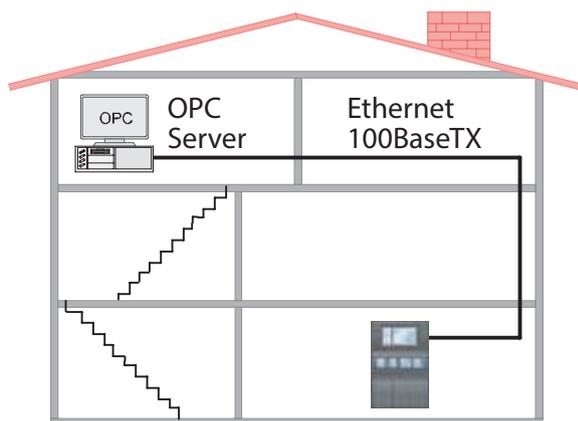


Рис. 4.1: Подключение к BIS через OPC-сервер

#### Дополнительная информация в случае использования OPC-сервера

OPC-серверы в вашей сети должны быть добавлены в ПО конфигурирования FSP-5000-RPS.

В программном обеспечении FSP-5000-RPS и на OPC-сервере необходимо выполнить следующие настройки:

- Сетевые узлы
- Сетевая группа
- RSN
- IP-адрес
- Порт

По умолчанию OPC-сервер использует порт 25000.

#### Замечание!

EN 54

Подключение к системе управления зданием (например, BIS) через интерфейс Ethernet и OPC-сервер или FSI-сервер совместимо с EN54, только если функции EN54 выполняются исключительно пожарной панелью. Любые связанное с EN54 управление или администрирование (например, управление оповещателями или администрирование отключения) системы управления зданием требует индивидуальной EN54-сертификации всей системы органом сертификации.



**Замечание!**

Программа конфигурирования FSP-5000-RPS

Необходимо назначить OPC-сервер всем сетевым узлам, с которых требуется передавать статусы.

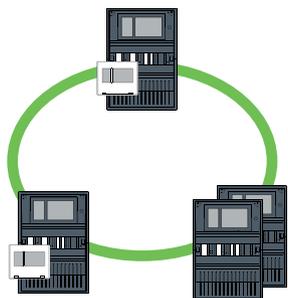
**4.1****Кольцо CAN**

Рис. 4.2: Кольцо CAN

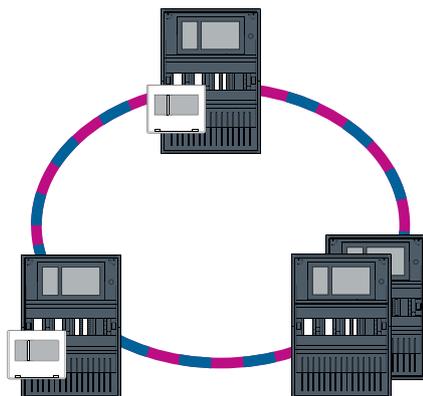
**4.2****Кольцо Ethernet**

Рис. 4.3: Кольцо Ethernet

**4.3****Кольцо Ethernet с OPC-сервером****Коммутатор Ethernet для подключения OPC-сервера необходимо запрограммировать отдельно**

Программирование IP-адреса и настроек резервирования коммутатора Ethernet см. в разделе *Настройка коммутатора*, Страница 45. 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.

**OPC-сервер необходимо запрограммировать отдельно**

Программирование IP-адреса, сетевых узлов, сетевой группы и RSN. См. соответствующий раздел в главе «Установка» Руководства по сетевым подключениям.

По умолчанию OPC-сервер использует порт 25000.

Убедитесь в идентичности настроек ПО конфигурирования FSP-5000-RPS и OPC-сервера.

**Параметры**

- OPC-сервер может быть подключен с помощью оптоволоконного или Ethernet-кабеля (медного).

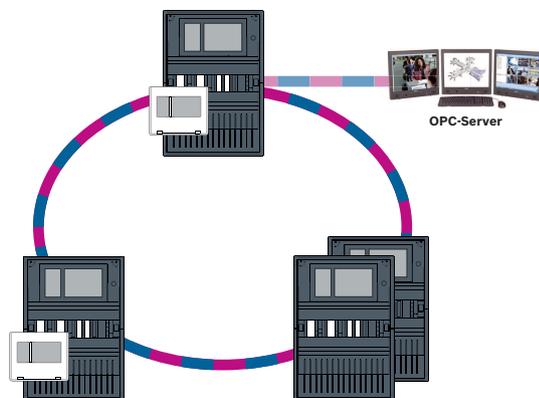


Рис. 4.4: Кольцо Ethernet с OPC-сервером

#### 4.4 Кольцо Ethernet с OPC-сервером к резервной панели

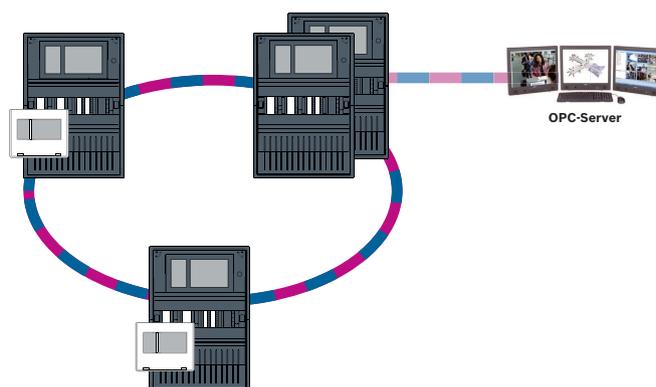


Рис. 4.5: Кольцо Ethernet с OPC-сервером к резервной панели

#### 4.5 Двойное кольцо Ethernet/CAN

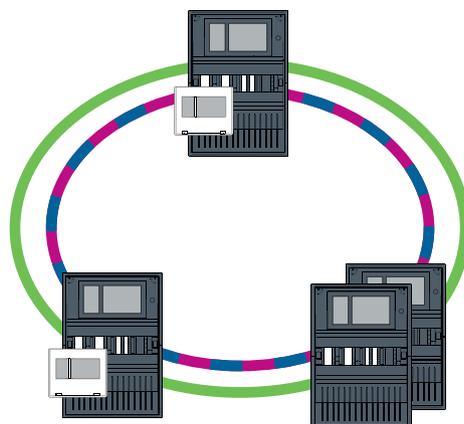


Рис. 4.6: Двойное кольцо Ethernet и CAN

#### 4.6 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.

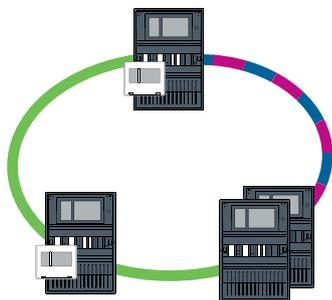


Рис. 4.7: Кольцо CAN с сегментами Ethernet

## 4.7

### 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 магистральной 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 14.



#### Замечание!

Эта топология требует дополнительной настройки всех RSTP-коммутаторов в магистральной. 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 точек обнаружения.

Это ограничение не применимо в кольцевой подсети Ethernet, так как функцию резервирования выполняют подключенные к данным двум кольцам коммутаторы.

#### Дополнительные параметры

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



#### Замечание!

Для всех RSTP-коммутаторов в магистральной следует задать более высокий RSTP-приоритет, чем в подсетях. В результате корневой мост RSTP всегда останется в магистральной, даже в случае отказа.

RSTP-коммутаторы для кольцевых подсетей — часть магистральной!

В магистральной используйте RSTP-приоритет 16384.



#### Замечание!

Чем меньше заданное значение, тем выше RSTP-приоритет.

**Коммутаторы для подключения OPC-сервера и кольцевых подсетей должны настраиваться отдельно**

Программирование IP-адреса и настроек резервирования коммутаторов Ethernet см. в разделе *Настройка коммутатора, Страница 45*. В случае этой топологии выходы неисправности коммутатора должны использоваться только при наличии резервного источника питания для коммутатора или соединения между коммутаторами. См. раздел *Коммутатор Ethernet, Страница 56*.

Убедитесь в идентичности настроек RSTP в контроллерах панели, FSP-5000-RPS и коммутаторе Ethernet.

**Замечание!**

Измените RSTP-приоритет для RSTP-коммутаторов, соединяющих кольца, так как они принадлежат к магистрали.

**OPC-сервер необходимо запрограммировать отдельно.**

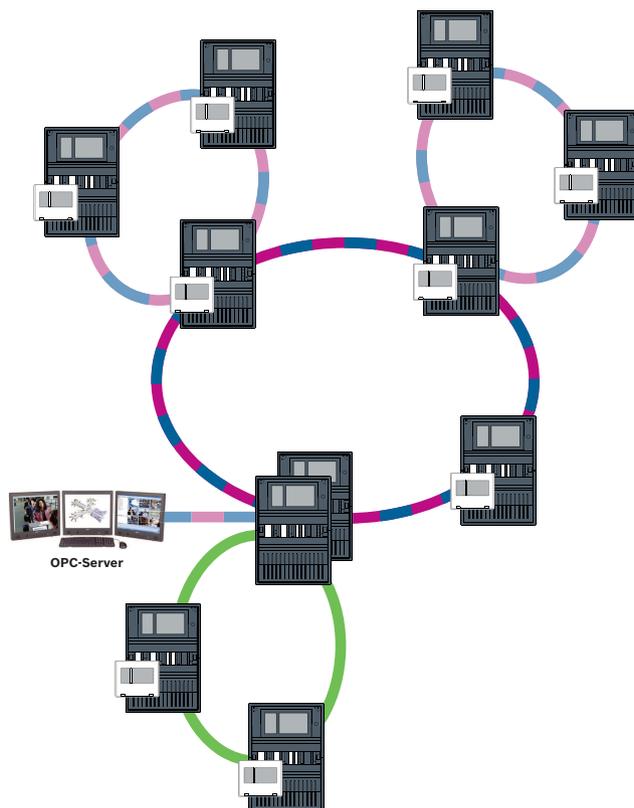
Программирование IP-адреса, сетевых узлов, сетевой группы и RSN см. в разделе *OPC-серверы, Страница 62*.

По умолчанию OPC-сервер использует порт 25000.

Убедитесь в идентичности настроек ПО конфигурирования RPS и OPC-сервера.

**Параметры**

- OPC-сервер может быть подключен с помощью оптоволоконного или Ethernet-кабеля (медного).



**Рис. 4.8:** Магистраль Ethernet с кольцевыми подсетями

## 4.8 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.

### Коммутаторы для соединения OPC-сервера и второго кольца должны программироваться отдельно

Программирование IP-адреса и настроек резервирования коммутатора Ethernet см. в разделе *Настройка коммутатора, Страница 45*. В случае этой топологии выходы неисправностей коммутатора должны использоваться только при наличии резервного источника питания для коммутатора. См. раздел *Коммутатор Ethernet, Страница 56*. 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.

### OPC-сервер необходимо запрограммировать отдельно

Программирование IP-адреса, сетевых узлов, сетевой группы и RSN. См. соответствующий раздел в главе «Установка» Руководства по сетевым подключениям.

По умолчанию OPC-сервер использует порт 25000.

Убедитесь в идентичности настроек ПО конфигурирования FSP-5000-RPS и OPC-сервера.

### Параметры

- OPC-сервер может быть подключен с помощью оптоволоконного или Ethernet-кабеля (медного).

В этих примерах кольцо a — магистраль. Кольцевой шлейф b — кольцевая подсеть.

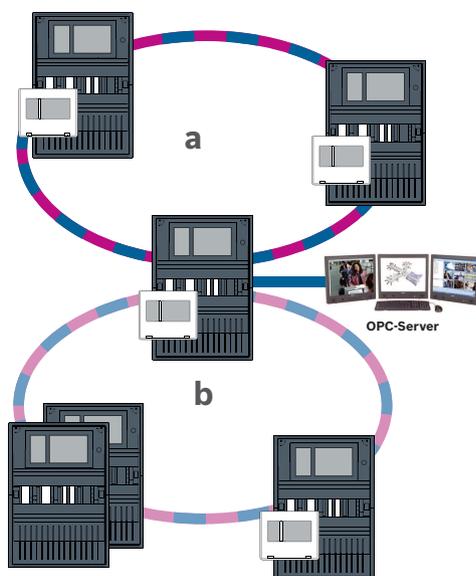


Рис. 4.9: Подключение кольца Ethernet через панель без резервирования

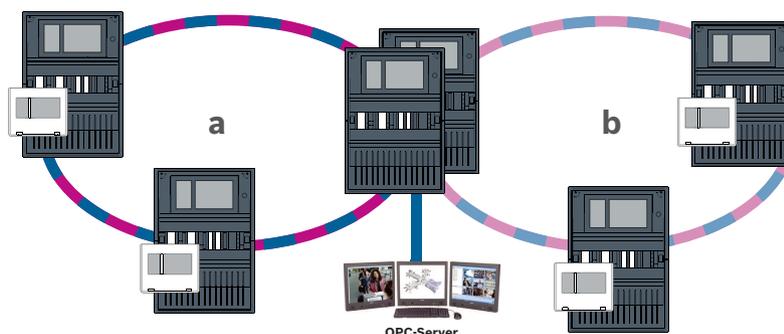


Рис. 4.10: Подключение кольца Ethernet через резервную панель

## 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 OPC, FSM-5000-FSI, Praesideo/PAVIRO или UGM-2040 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, ETH4 можно использовать для подключения OPC, FSM-5000-FSI, Praesideo/PAVIRO, или UGM-2040
4. Если подключение панелей не осуществляется через ETH1 и ETH2, каждый из них можно использовать для подключения OPC, FSM-5000-FSI, Praesideo/PAVIRO или UGM-2040

## 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 восстановлении соединения.

## 5.2 Диаметр сети

Диаметр Ethernet-сетей панелей RSTP не должен превышать 32.

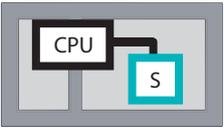
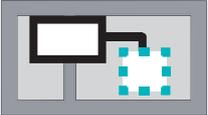
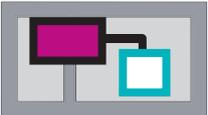
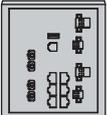
### Описание

Диаметр сети соответствует количеству RSTP-коммутаторов на самом длинном участке без петель между любыми двумя конечными точками в сети.

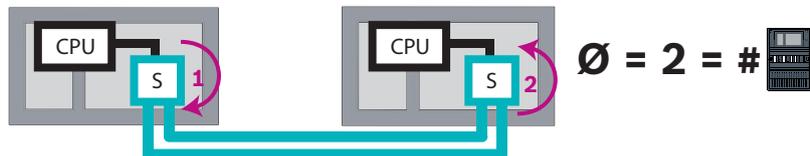
В отношении Ethernet-сети панелей RSTP следует учитывать следующее:

- 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 OPC-серверов.

**Ключ**

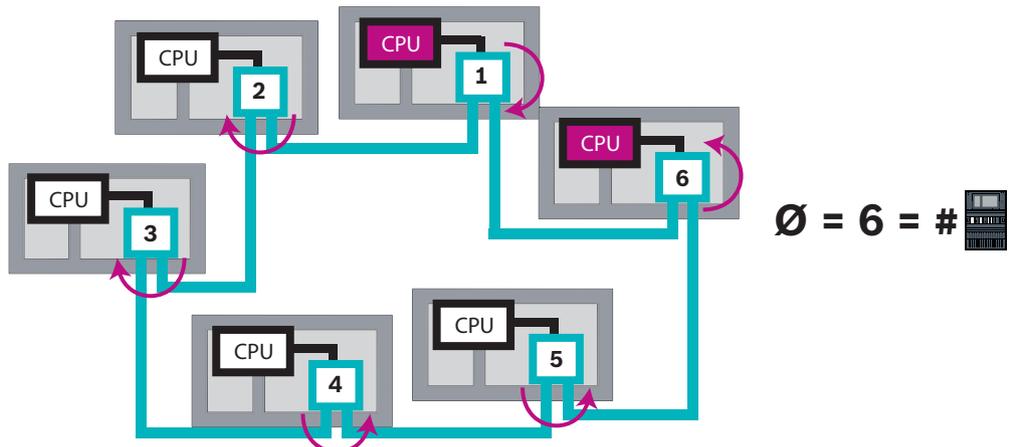
	Центральный процессор в контроллере панели или на удаленной клавиатуре.
	Внутренний коммутатор RSTP в контроллере панели или на удаленной клавиатуре.
	Контроллер панели или удаленная клавиатура с центральным процессором и внутренним коммутатором RSTP.
	Резервный контроллер панели с центральным процессором 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.



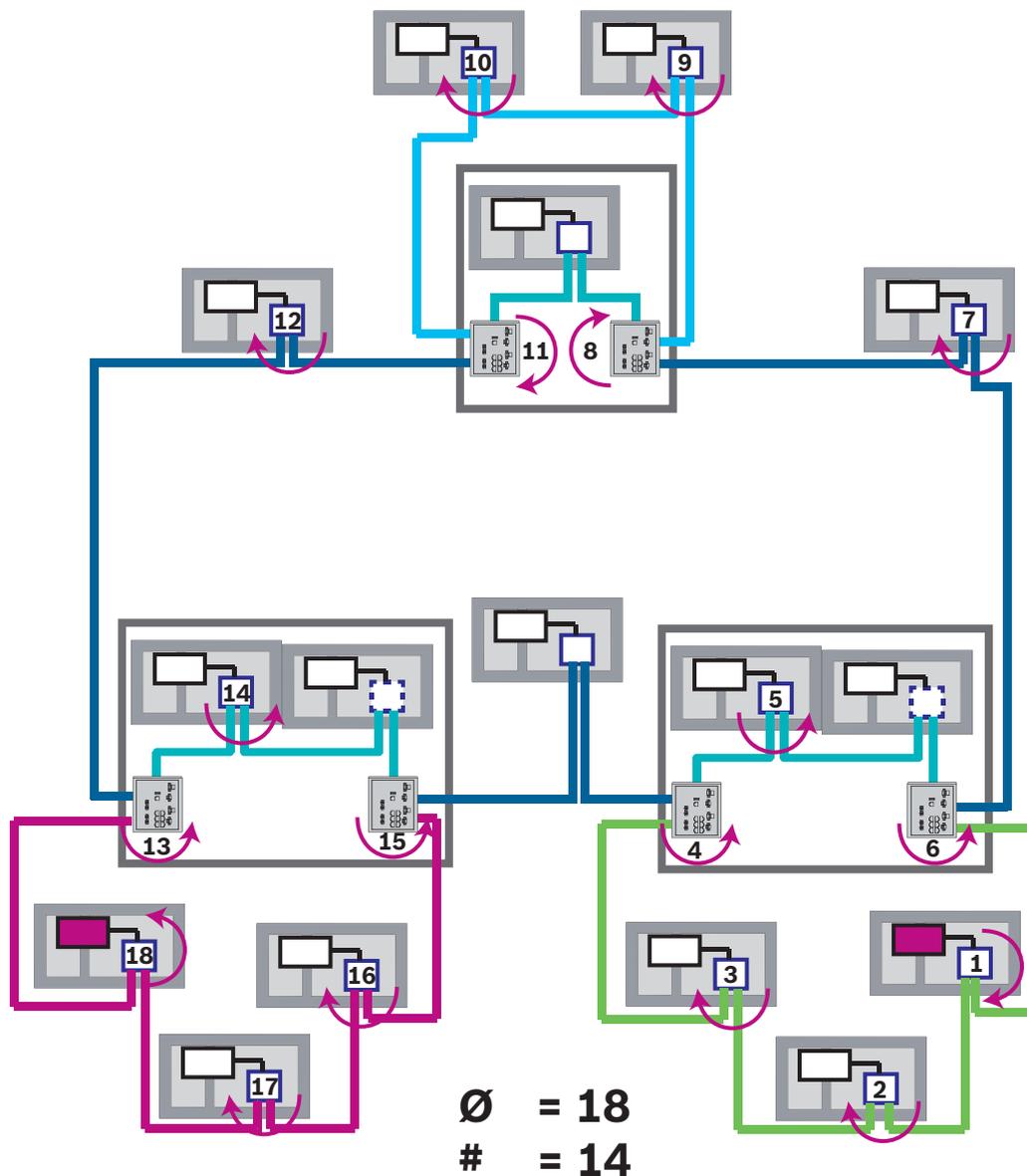
**Рис. 5.1:** Сетевой диаметр кольца с 2 панелями

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 магистральной сети с кольцевыми подсетями

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

## 5.3

### Используемые кабели

Для организации сетей 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 50/125 $\mu$  или I-VH2G 62.5/125 $\mu$ , заглушка SC.  
Одномодовый: оптоволоконный экранированный Ethernet-кабель, дуплекс I-VH2E 9/125 $\mu$ , 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

В соответствии с требованиями VdS 2540 использовать в качестве путей передачи данных следует оптоволоконный кабель для подключений Ethernet. Для подключений внутри корпуса можно использовать кабели Ethernet TX.

## 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 OPC, FSM-5000-FSI, Praesideo/PAVIRO или UGM-2040 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, ETH4 можно использовать для подключения OPC, FSM-5000-FSI, Praesideo/PAVIRO, или UGM-2040
4. Если подключение панелей не осуществляется через ETH1 и ETH2, каждый из них можно использовать для подключения OPC, FSM-5000-FSI, Praesideo/PAVIRO или UGM-2040

#### 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 запрограммировать 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.

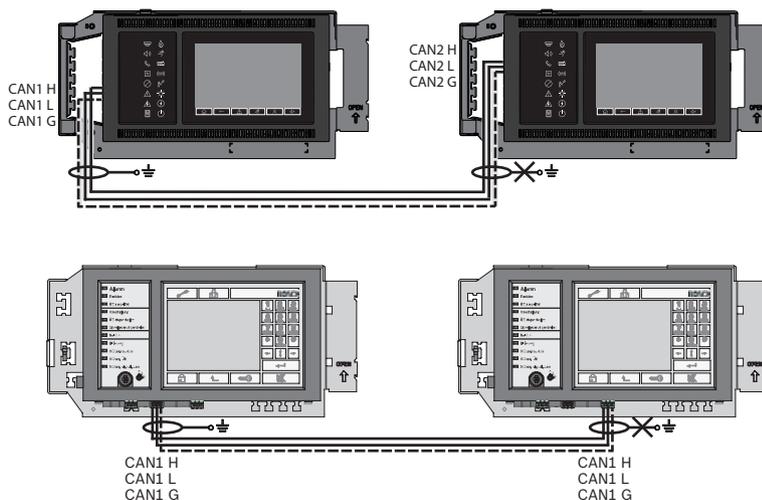


Рис. 6.1: Подключение CAN (вверху: AVENAR, внизу: FPA)

### Длина кабеля для сетевого подключения

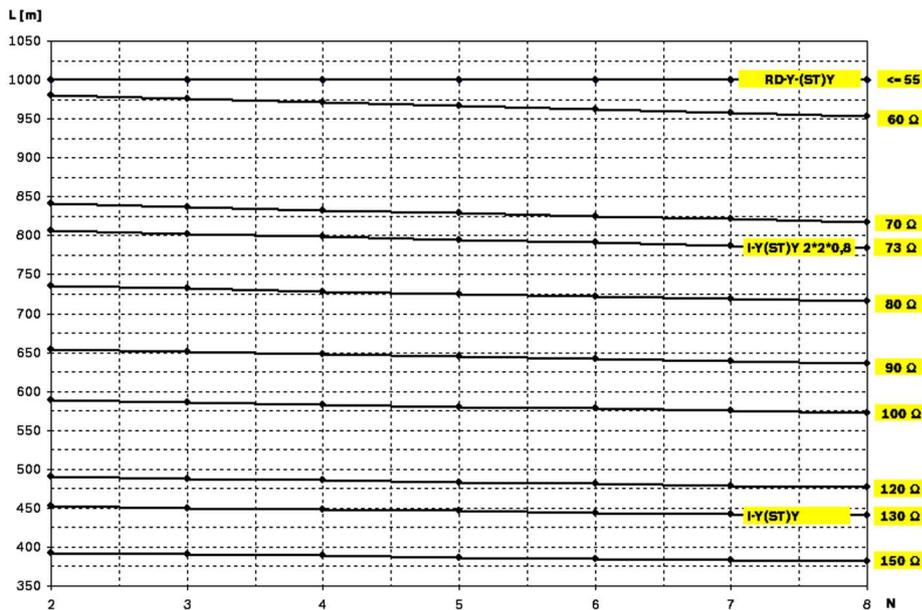
Максимально допустимая длина кабеля зависит от контурного сопротивления используемого кабеля и числа узлов, обменивающихся данными.

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



### 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.

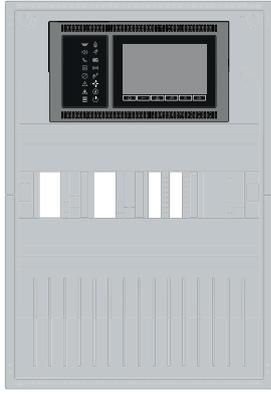
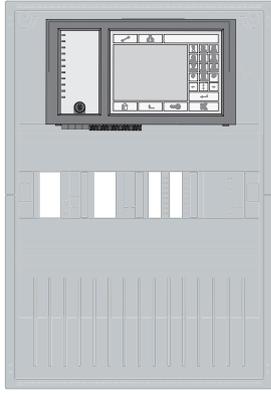
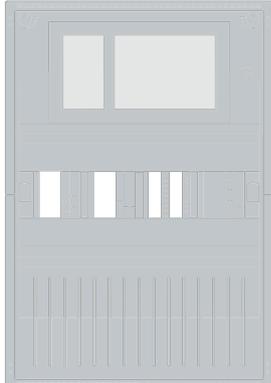
### Процедура создания сети CAN

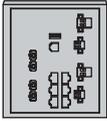
1. Создайте план сети.
2. Создайте сеть в FSP-5000-RPS.
3. Распечатайте информацию о сети или сохраните ее на ноутбуке.
4. Установите панели управления и подключите их к сети с помощью кабелей CAN.
5. Подключите компьютер к панели управления в сети с помощью программного обеспечения для программирования 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)

Значок	Описание
	<p>Кабель Ethernet TX или FX, длина кабеля TX между узлами &lt; 100 м</p>
	<p>Кабель CAN</p>
	<p>Корпус Примечание. Для упрощения представления различных схем сетевого подключения на рисунках в этой главе все панели обозначаются малыми корпусами панелей. Малый корпус может <b>не</b> 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.</p>
	<p>AVENAR panel</p>
	<p>FPA</p>
	<p>AVENAR panel или FPA</p>

Значок	Описание
	Коммутатор Ethernet в качестве внешнего RSTP-коммутатора (или универсальный коммутатор Ethernet MM)
	Медиаконвертер
	Защищенный сетевой шлюз для Remote Services
	Подключение к OPC-серверу, FSM-5000-FSI, Praesideo/PAVIRO или UGM-2040

## 7.1 Ethernet-сеть панелей

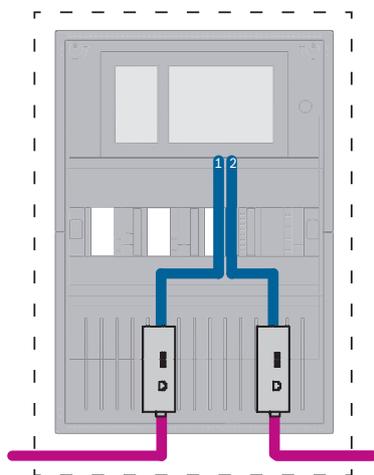


Рис. 7.1: Ethernet-сеть панелей

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

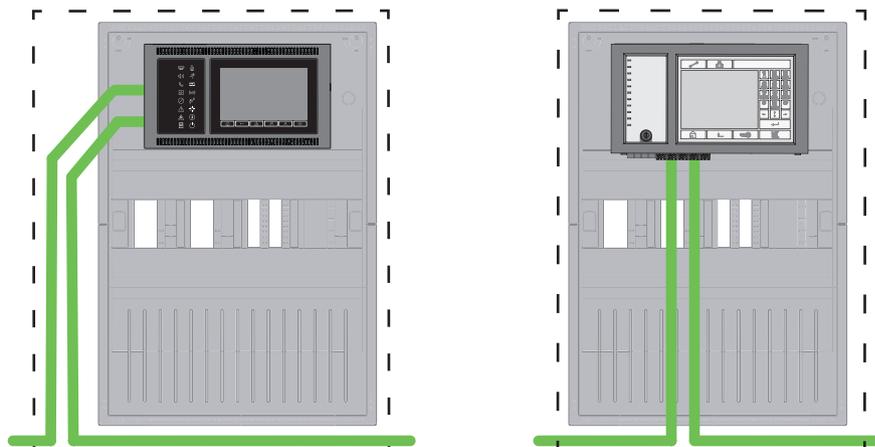
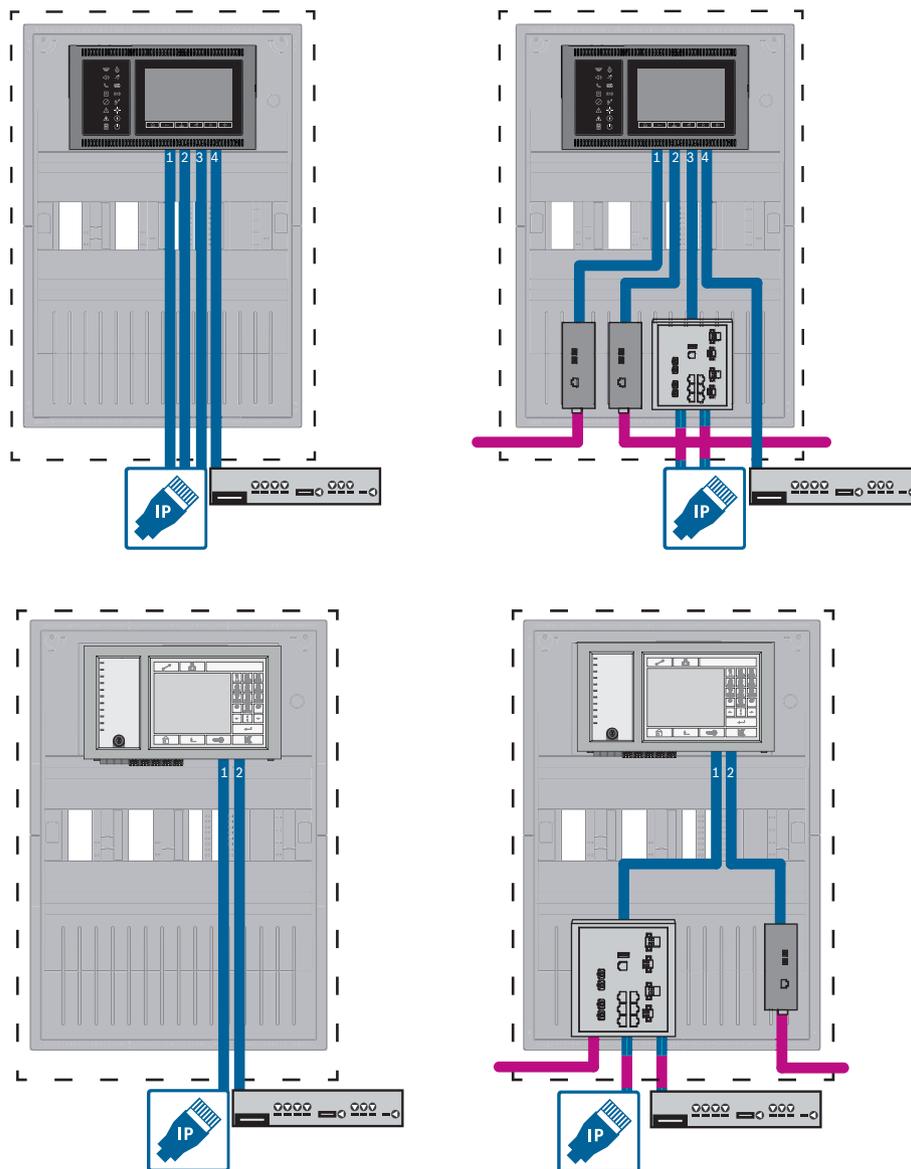


Рис. 7.2: CAN-сеть панелей

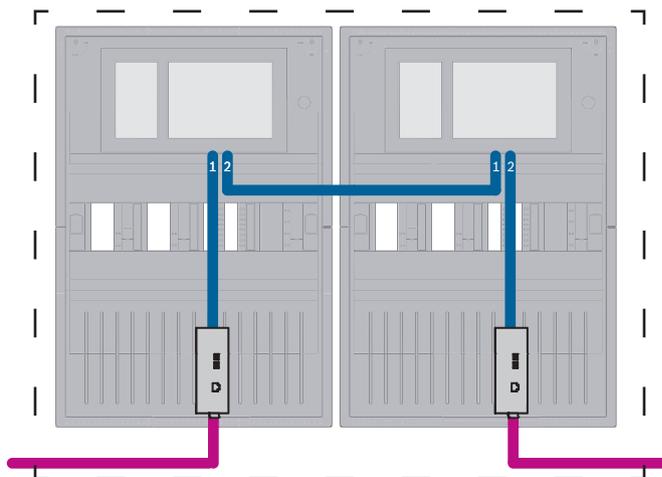
### 7.3 Подключение служб к панели



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

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

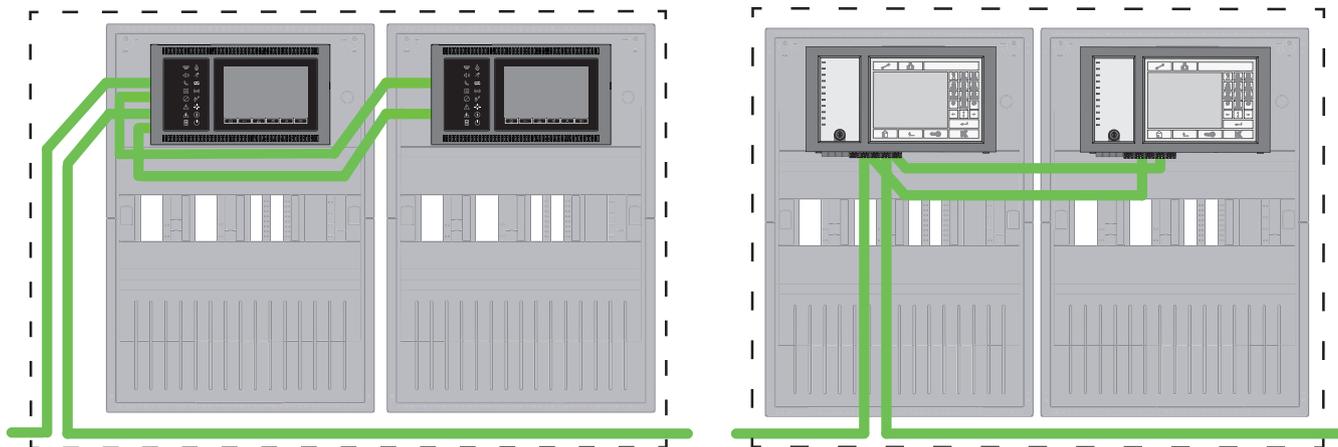
## 7.4 Ethernet-сеть панелей с резервными панелями



**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

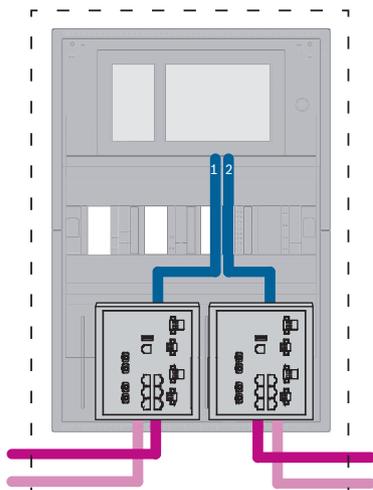


Рис. 7.6: Подключение сетей Ethernet

## 7.7 Сеть панелей с двумя кольцами Ethernet и резервными панелями

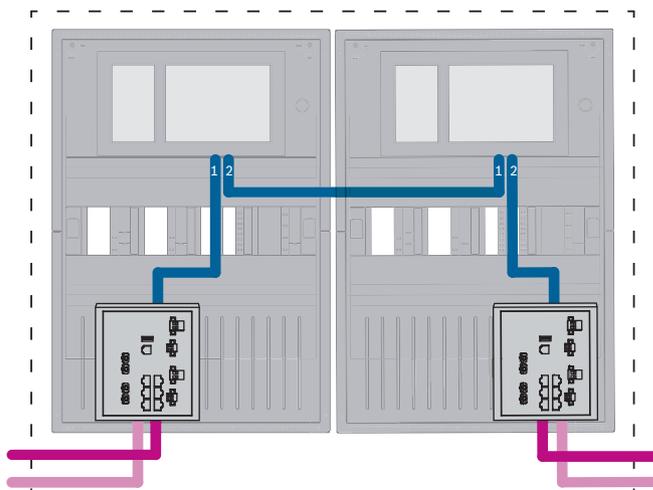


Рис. 7.7: Подключение Ethernet-сетей с резервными панелями

## 7.8 Подключение Ethernet- и CAN-среды с резервными панелями

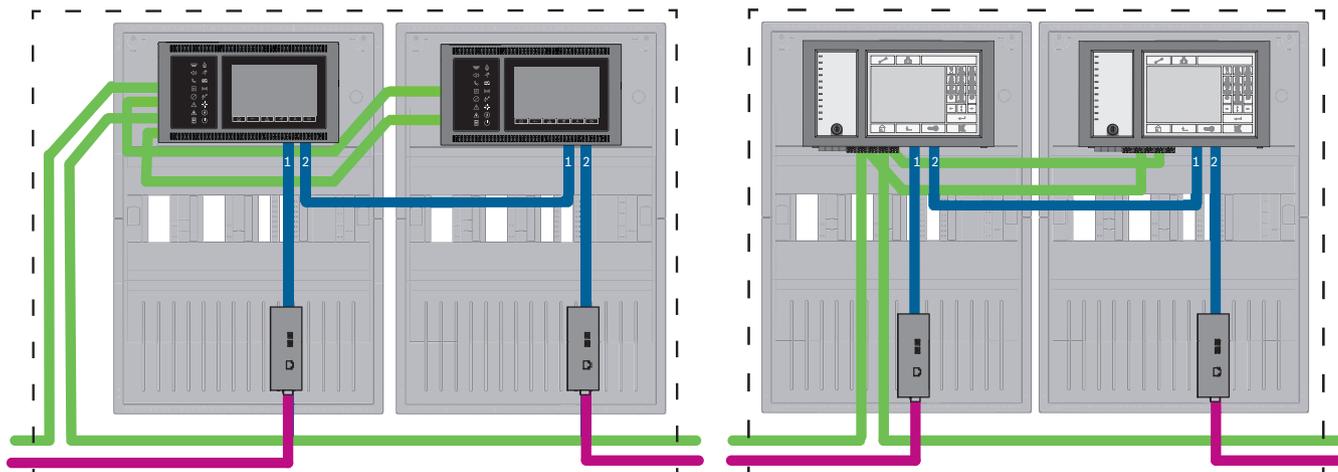


Рис. 7.8: Подключение Ethernet- и CAN-среды с резервными панелями

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

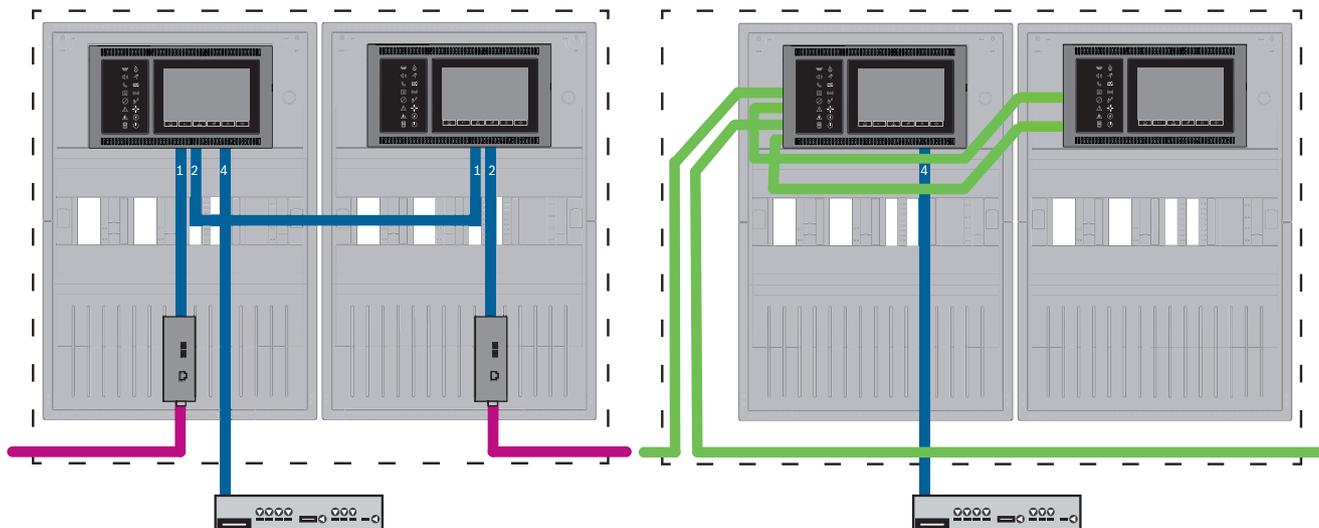




Рис. 7.9: Левая сторона: в сети Ethernet; правая сторона: в сети CAN

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

## 8 Службы Remote Services

Remote Services включают следующие службы:

- Remote Connect
- Remote Alert
- Remote Maintenance

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

### 8.1 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.

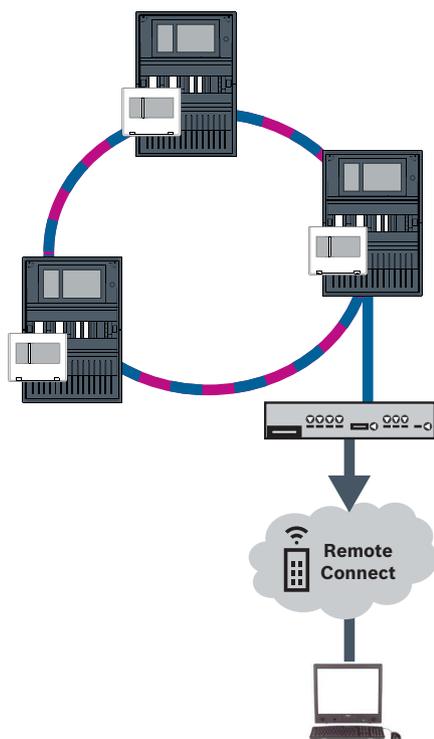
В случае сети панелей одна из панелей в сети должна быть подключена к защищенному сетевому шлюзу. Единственно, это подключение должно быть выделенным подключением Ethernet.



**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.

Необходимо включить Remote Connect в конфигурации FSP-5000-RPS этой панели. В приведенной топологии показаны контроллеры панели, подключенные через Ethernet, где защищенный сетевой шлюз соединен с сетью через коммутатор Ethernet (как правило, MM).



**Рис. 8.1:** Remote Connect в кольце Ethernet



**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 отдельные 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.



В следующей топологии показана сеть CAN, где защищенный сетевой шлюз соединен с сетью через порт Ethernet.

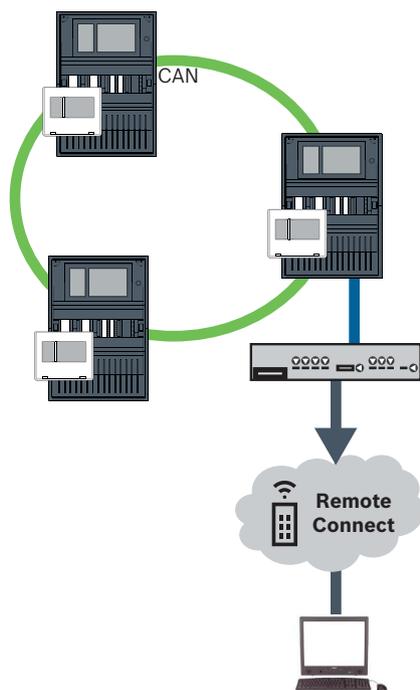


Рис. 8.2: Remote Connect в кольце CAN

## 8.2

### Remote Alert

С помощью Remote Alert панель отправляет соответствующую информацию о статусе на портал Remote Portal.

Передаваемые данные анализируются с помощью Remote Alert. В случае непредвиденного события пользователь получает уведомление о возникших оповещениях по SMS или электронной почте.

Remote Alert также доступна для Private Secure Network.

## 8.3 Remote Maintenance

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

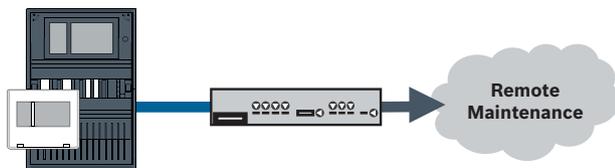


Рис. 8.3: Remote Maintenance



### 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.



### Замечание!

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

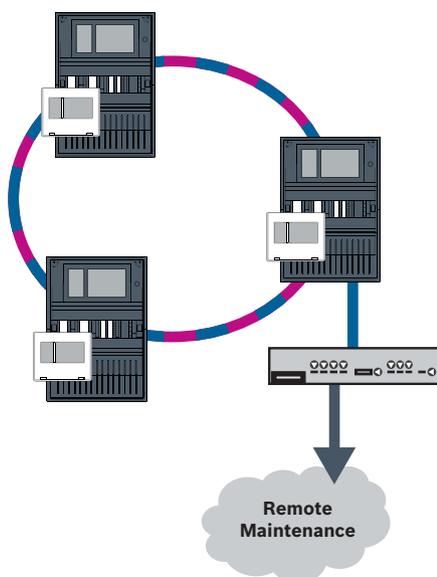


Рис. 8.4: Remote Maintenance

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 для Remote Portal

Remote Maintenance собирает данные о соответствующих устройствах и функциональных модулях LSN и отправляет их на портал Remote Portal, где они анализируются и визуализируются для выполнения обслуживания.

### 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).

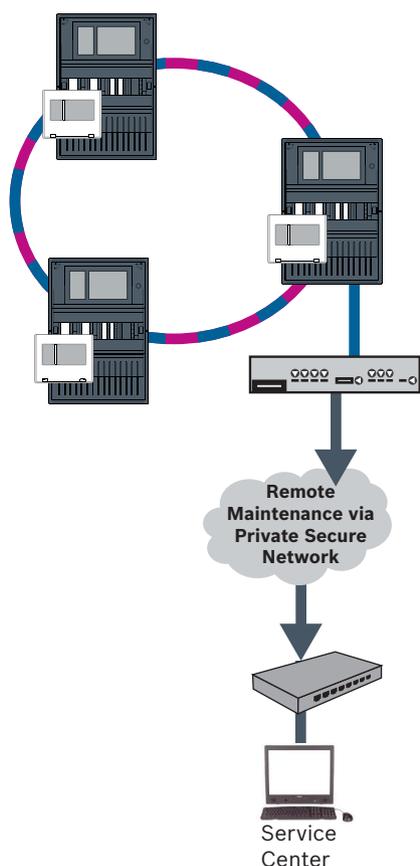
**Внимание!**

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.

**Замечание!**

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



**Рис. 8.5:** 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 45*. 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.

## 8.4 Remote Portal

### Требования



#### 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 4.8 или выше и доступом к Интернету



#### Замечание!

Избегайте обновления защищенного сетевого шлюза во время подключения.

Обновления защищенного сетевого шлюза регулярно выполняются ранним утром.

Следовательно, необходимо указать часовой пояс в разделе **System** -> **General Settings** -> **Timezone**.

### Инструкции

Для использования Remote Services необходимо быть пользователем учетной записи Remote Portal.

#### Шаг 1. Создание учетной записи Remote Portal

Одной учетной записью Remote Portal могут пользоваться несколько пользователей. У каждой учетной записи Remote Portal есть один уникальный Remote ID, представляющий одну компанию. Если невозможно использовать существующую учетную запись Remote Portal, необходимо создать учетную запись:

1. На странице <https://remote.boschsecurity.com> -> **Sign Up** введите свое имя, название компании, адрес электронной почты и пароль. Ознакомьтесь с правилами и условиями и установите флажок **I agree to the terms and conditions**. Ознакомьтесь с заявлением о конфиденциальности и выберите **I agree to the privacy statement**.
2. Нажмите кнопку **Register**. Remote Portal вскоре отправит сообщение электронной почты со ссылкой для активации на указанный адрес.
3. Для активации учетной записи щелкните ссылку активации. На Remote Portal щелкните свое имя пользователя и выберите **Account Settings**. Здесь вы найдете свой Remote ID. Этот Remote ID вам потребуется позже для работы с контроллером панели.

Чтобы у каждого техника была своя учетная запись, можно создать несколько пользователей с одним Remote ID:

Вы подключены к Remote Portal.

- ▶ Выберите **Users** -> **New Technician**. Введите необходимые данные и подтвердите их, нажав кнопку **Save**.

#### Шаг 2. Подключите защищенный сетевой шлюз

Для работы Remote Services требуется использовать защищенный сетевой шлюз.

1. Подключите порт WAN защищенного сетевого шлюза к маршрутизатору для Интернета или сети компании, предоставляющей доступ к Интернету.
2. На интернет-маршрутизаторе или в корпоративной сети проверьте доступность следующих протоколов и портов для защищенного сетевого шлюза (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

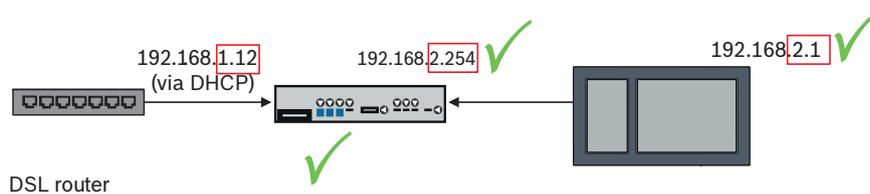
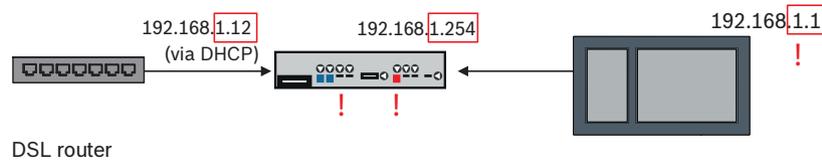
3. Подключите порт LAN1 защищенного сетевого шлюза к назначенному для этого Ethernet-порту контроллера панели, используя входящий в комплект сетевой кабель CAT5 RJ45. Изучите возможные топологии.
4. Подключите защищенный сетевой шлюз к сети питания с напряжением 100 V - 230 V, используя входящий в комплект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

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

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

**Разделение подсетей (выкл. индикатор VPN)**

Подключение защищенного сетевого шлюза к Remote Services не удастся 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 октет IP-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.

#### Шаг. Установление удаленного соединения

1. На панели используйте стандартные настройки Ethernet.
2. Перезапустите панель.
3. Для проверки подлинности выберите команду **Конфигурация** -> **Сетевые сервисы** -> **Изм. дату/время**, введите текущую дату и подтвердите настройки.
4. Выберите **Configuration** -> **Network Services** -> **Remote Services** и введите Remote ID. Можно проверить состояние удаленного соединения: выберите на контроллере панели пункт **Диагностика** -> **Сетевые сервисы** -> **Remote Services**.

#### Шаг 4. Назначение лицензии на Remote Portal

Чтобы использовать Remote Services, необходимо назначить лицензию на Remote Portal. Одна лицензия автоматически предоставляется учетной записи при успешном подключении в первый раз.



#### Замечание!

Уже назначенную лицензию переназначить или приостановить невозможно.

1. На странице <https://remote.boschsecurity.com> -> **Login** введите адрес электронной почты и пароль.
2. Выберите **Systems**.
3. Выберите систему.
4. В разделе **Services** нажмите кнопку **Add Service** под службой.
5. По умолчанию лицензия обновится автоматически (**Service Settings**, параметр **With Auto-Renew**).
6. Нажмите **Save**, чтобы подтвердить свои параметры.

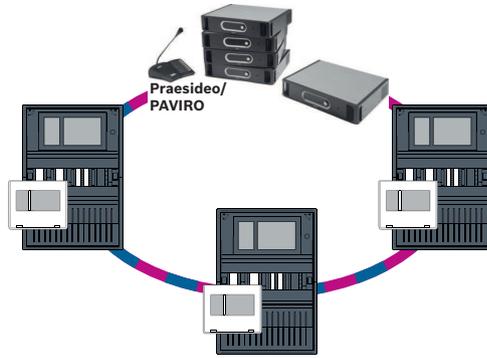
После назначения лицензии можно использовать соответствующую службу. Назначенная лицензия отмечена зеленым крючком.

#### Шаг 5. Перезаказ лицензии

1. Заказ годовых лицензий на системы пожарной сигнализации Bosch. Для каждой сети требуются собственные лицензии. Bosch отправляет электронное сообщение на указанный адрес. Сообщение содержит уникальные номера регистрации для всех заказанных лицензий, а также инструкция и ссылка на Remote Portal.
2. На странице <https://remote.boschsecurity.com> -> **Login** введите адрес электронной почты и пароль.
3. Выберите **Licenses**.
4. Нажмите кнопку **+**.
5. Выполните инструкции в окне **Add Licenses** и подтвердите выбор, нажав **Save**.
6. Список лицензий обновится.

## 9 Системы речевого и аварийного оповещения

В следующей топологии изображены контроллеры панели, подключенные через Ethernet, где система Praesideo/PAVIRO интегрирована в кольцо панелей с помощью интерфейса Ethernet.

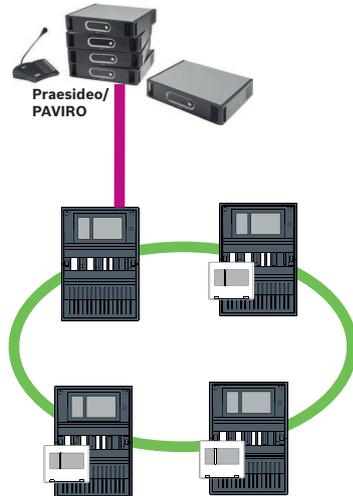


**Рис. 9.1:** Кольцо Ethernet с Praesideo/PAVIRO

Используйте Ethernet Switch (как правило, MM BPA-ESWEX-RSR20), утвержденный для использования с микропрограммой панели версии 2.8.

Чтобы заблокировать отправку соответствующего многоадресного трафика EN 54-2 в систему Praesideo/PAVIRO, активируйте отслеживание IGMP для MM, см. соответствующий раздел главы «Установка» Руководства по сетевым подключениям.

К любому контроллеру панели сети CAN можно подключить одну систему Praesideo/PAVIRO с использованием интерфейса Ethernet. В приведенной топологии показаны контроллеры панели, подключенные через CAN, и система Praesideo/PAVIRO, подключенная к одному из контроллеров с помощью интерфейса Ethernet.



**Рис. 9.2:** Подключение Praesideo/PAVIRO к сети CAN



**Замечание!**

Так как трафик сети CAN не будет передаваться через данное соединение Ethernet, в программе настройки FSP-5000-RPS необходимо отключить сетевое подключение через IP.

Если оно не отключено, данная сеть не будет соответствовать EN 54.



**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 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.

### 10.1 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 BSM.



#### 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 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.

Обратите внимание на минимальные радиусы сгиба, указанные в технических характеристиках на кабель.



#### 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!**

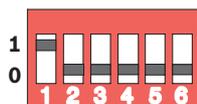
Максимальная секция передачи для многомодовых преобразователей среды через FX: 2000 м.

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.

## 10.2

### Установка Ethernet-коммутатора

**Предупреждение!**

Лазерный источник света

Не смотрите на источник луча невооруженным глазом или через любые оптические приборы (например, увеличительное стекло, микроскоп). Невыполнение этого требования опасно для глаз при расстояниях менее 100 мм. Свет выходит из зрительных терминалов и на концах подключенных к ним оптоволоконных кабелей. 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).

## 10.3

### 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 46,
- Задать настройки резервирования, Страница 47.

Оptionальные настройки, например:

- Настройка реле отказа, Страница 47,
- Настройка контроля подключений, Страница 48,
- Активация отслеживания IGMP, Страница 48.

### 10.3.1

#### 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**.

### 10.3.2 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: используйте те же параметры, что и для контроллеров панели.

Щелкните **Write (Записать)**.

#### Замечание!

Настройки в отдельных пунктах меню конфигурации коммутатора вступают в силу после нажатия **Write (Записать)**.

Настройки сохраняются только постоянно, например, они сохраняются даже после перезапуска устройства, если в меню **Basic Settings (Основные параметры) -> Load/Save (Загрузить/Сохранить)** в поле **Save (Сохранить)** выбрать пункт **On the device (В устройстве)** и нажать кнопку **Save (Сохранить)**.



### 10.3.3 Настройка реле отказа

#### Замечание!

Реле неисправности требуется программировать только для приложений, для которых выполняется хотя бы одно из следующих требований:

Есть соединение между двумя устройствами switch. 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**.

**10.3.4****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)**.

Щелкните **Write (Записать)**.

**Замечание!**

Настройки в отдельных пунктах меню конфигурации коммутатора вступают в силу после нажатия **Write (Записать)**.

Настройки сохраняются только постоянно, например, они сохраняются даже после перезапуска устройства, если в меню **Basic Settings (Основные параметры) -> Load/Save (Загрузить/Сохранить)** в поле **Save (Сохранить)** выбрать пункт **On the device (В устройстве)** и нажать кнопку **Save (Сохранить)**.

**10.3.5****Приоритет QoS, только для UGM-2040**

Если коммутаторы используются для обеспечения связи между сетями FPA и UGM-2040, в коммутаторах UGM необходимо задать приоритет QoS.

В меню QoS/Priorität -> Global измените настройки поля раскрывающегося списка в Trusted Mode на trustIpDscp.

Щелкните **Write (Записать)**.

**Замечание!**

Настройки в отдельных пунктах меню конфигурации коммутатора вступают в силу после нажатия **Write (Записать)**.

Настройки сохраняются только постоянно, например, они сохраняются даже после перезапуска устройства, если в меню **Basic Settings (Основные параметры) -> Load/Save (Загрузить/Сохранить)** в поле **Save (Сохранить)** выбрать пункт **On the device (В устройстве)** и нажать кнопку **Save (Сохранить)**.

**10.3.6****Активация отслеживания IGMP**

Чтобы предотвратить передачу относящегося к EN 54-2 многоадресного трафика в другие системы, подключенные к Ethernet Switch (Praesideo/PAVIRO, 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.

## 10.4

### 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 USB составляет 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 -> Исполз. 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:

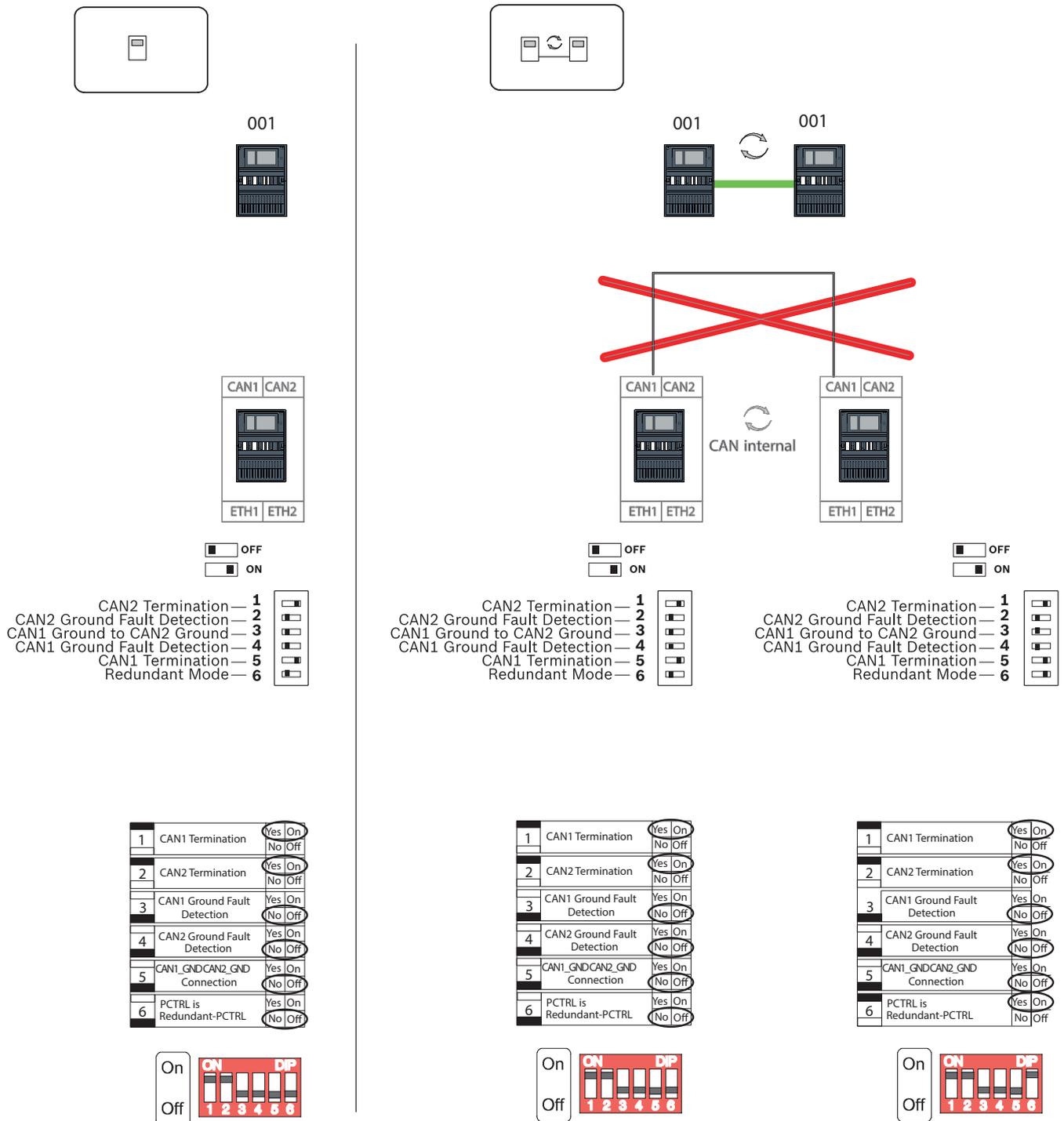
- ▶ На механических поворотных переключателях в задней части панели установите номер RSN и убедитесь, что он отображается на табличке под поворотными переключателями.

#### Конструкция топологии

Коммутаторы DIP для конфигурации разных топологий находятся сзади.

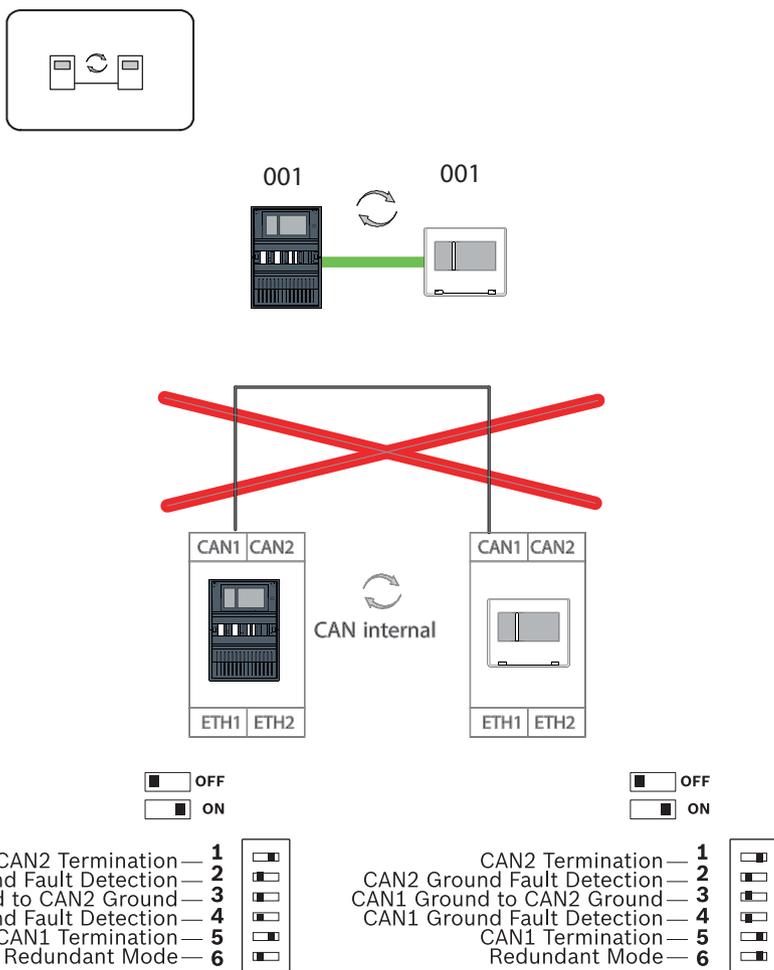
- ▶ Пометьте выбранные параметры на табличке рядом с коммутаторами DIP.

**Автономная панель и автономная панель с резервированием**



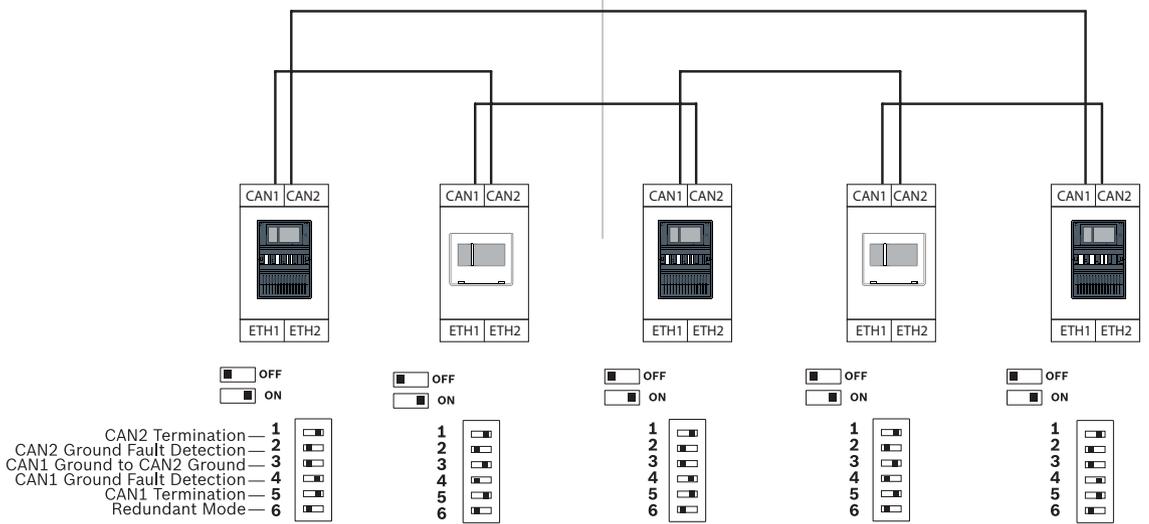
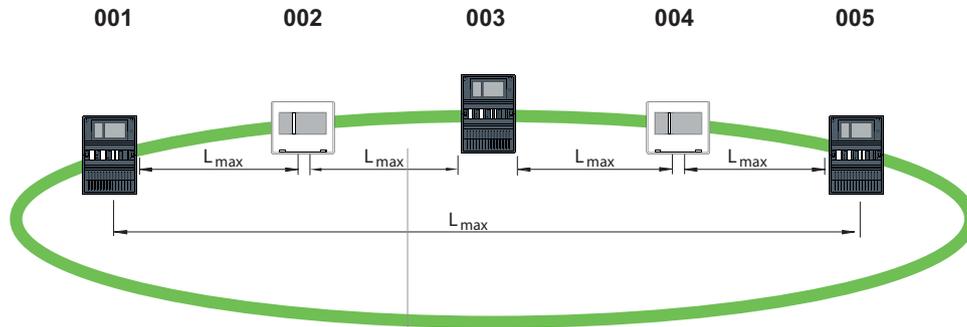
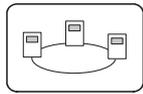
**Рис. 10.1:** Настройки DIP-переключателя для автономной панели (вверху: AVENAR, внизу: FPA, слева: обычная, справа: с резервированием)

### Удаленная клавиатура в качестве резервной панели



**Рис. 10.2:** Настройки DIP-переключателя для удаленной клавиатуры в качестве резервной панели (только AVENAR)

**Кольцо**



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

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

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

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

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

**Рис. 10.3:** Настройки DIP-переключателей для кольцевой топологии (вверху: AVENAR, внизу: FPA)

Кольцо с резервными панелями

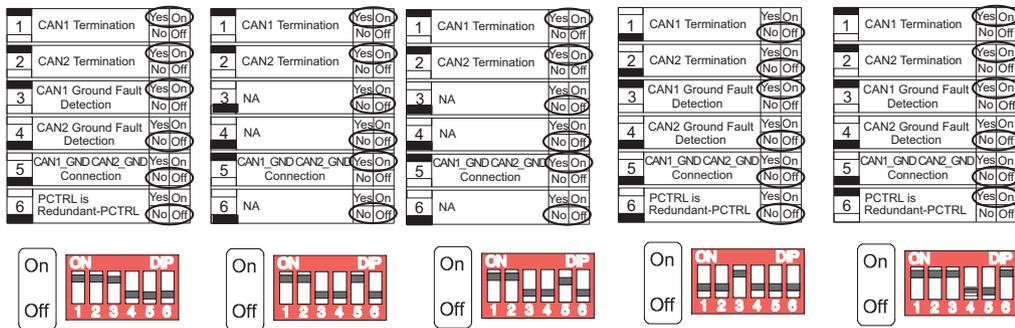
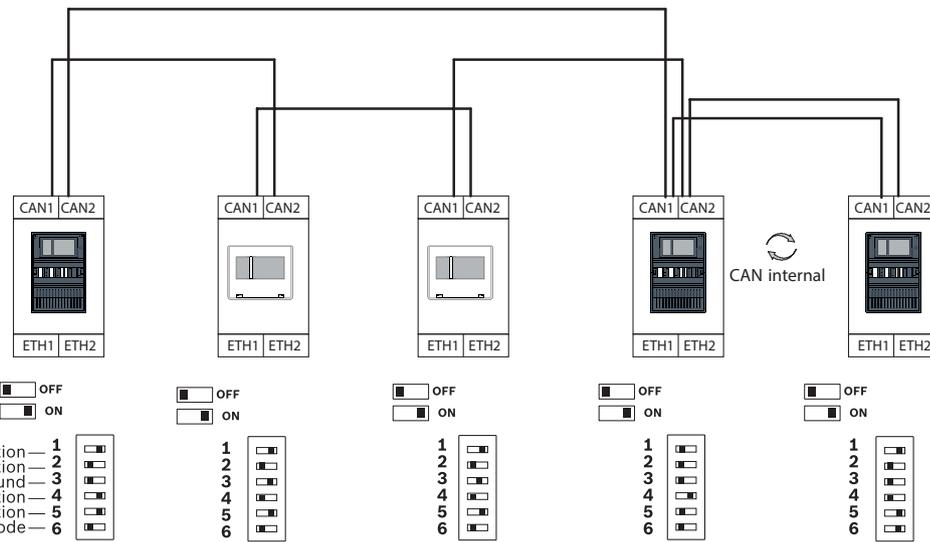
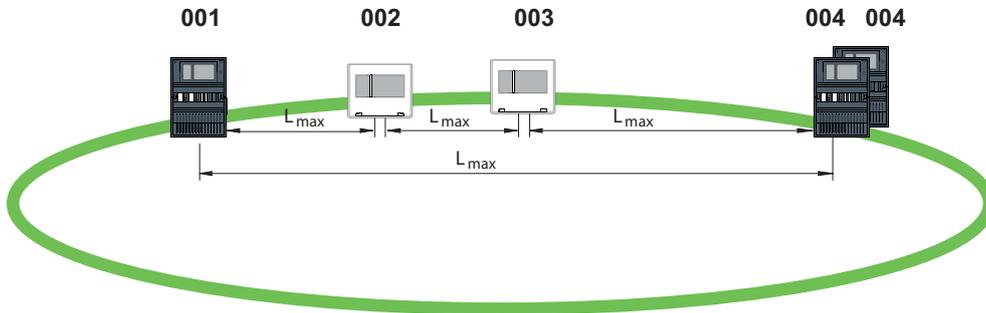
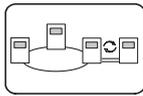


Рис. 10.4: Настройки DIP-переключателей для кольцевой топологии с резервными панелями (вверху: AVENAR, внизу: FPA)

### Кольцевая топология с удаленной клавиатурой в качестве резервной панели

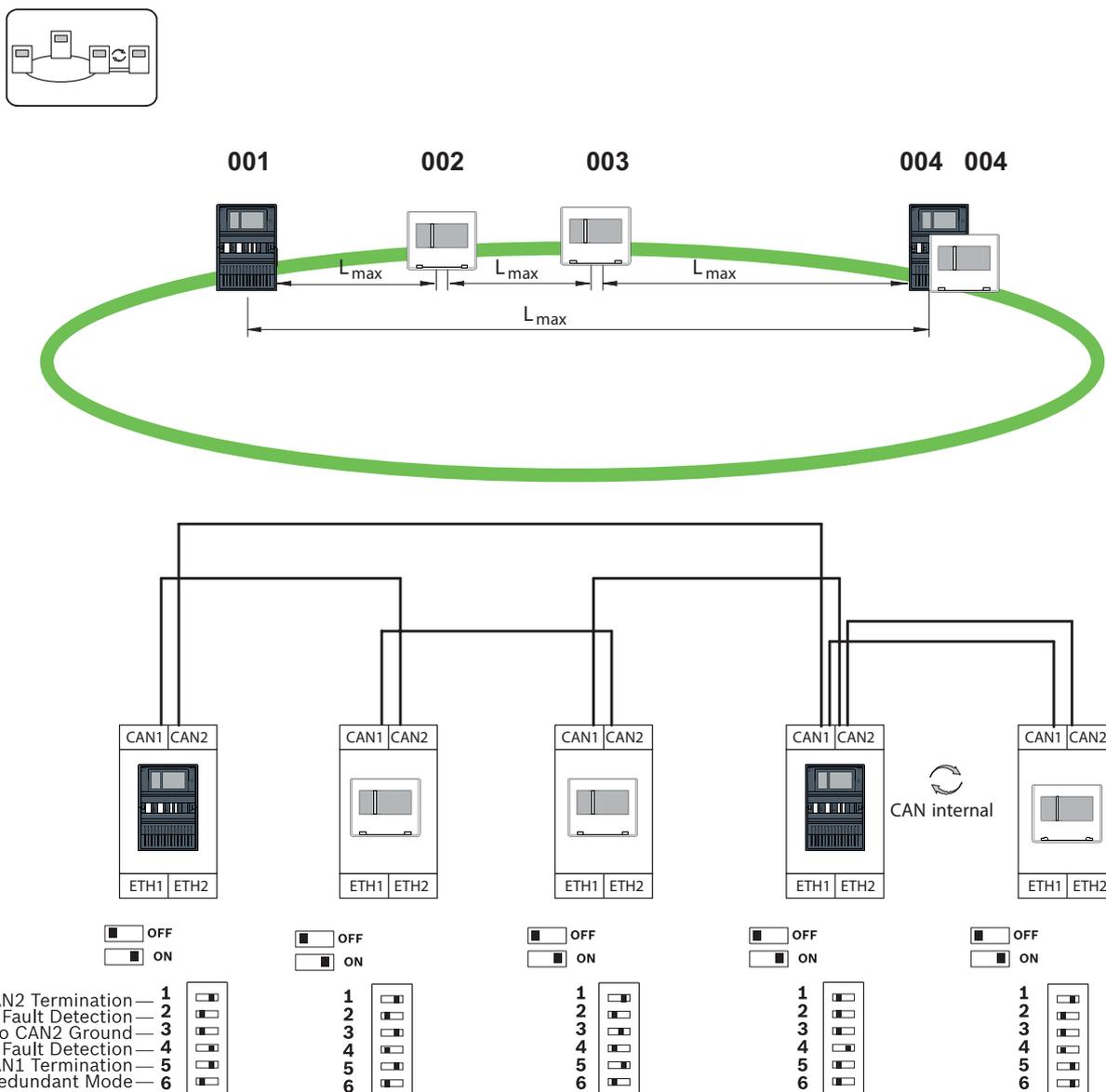


Рис. 10.5: Настройки DIP-переключателя для кольцевой топологии с удаленной клавиатурой (только AVENAR)

## 11 Кабельная сеть

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 системы BCM 0000 В или 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 А.
- 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 следует использовать лишь следующие кабели:

Кабель Ethernet

Экранированный Ethernet-кабель CAT5e или выше.

Обратите внимание на минимальные радиусы сгиба, указанные в технических характеристиках на кабель.

Опволоконный кабель

Многомодовый: опволоконный Ethernet-кабель, дуплекс I-VN2G 50/125μ или дуплекс I-VN2G 62.5/125μ, разъем SC.

Одномодовый: опволоконный Ethernet-кабель, дуплекс I-VN2E 9/125μ, разъем SC.

Обратите внимание на минимальные радиусы сгиба, указанные в технических характеристиках на кабель.

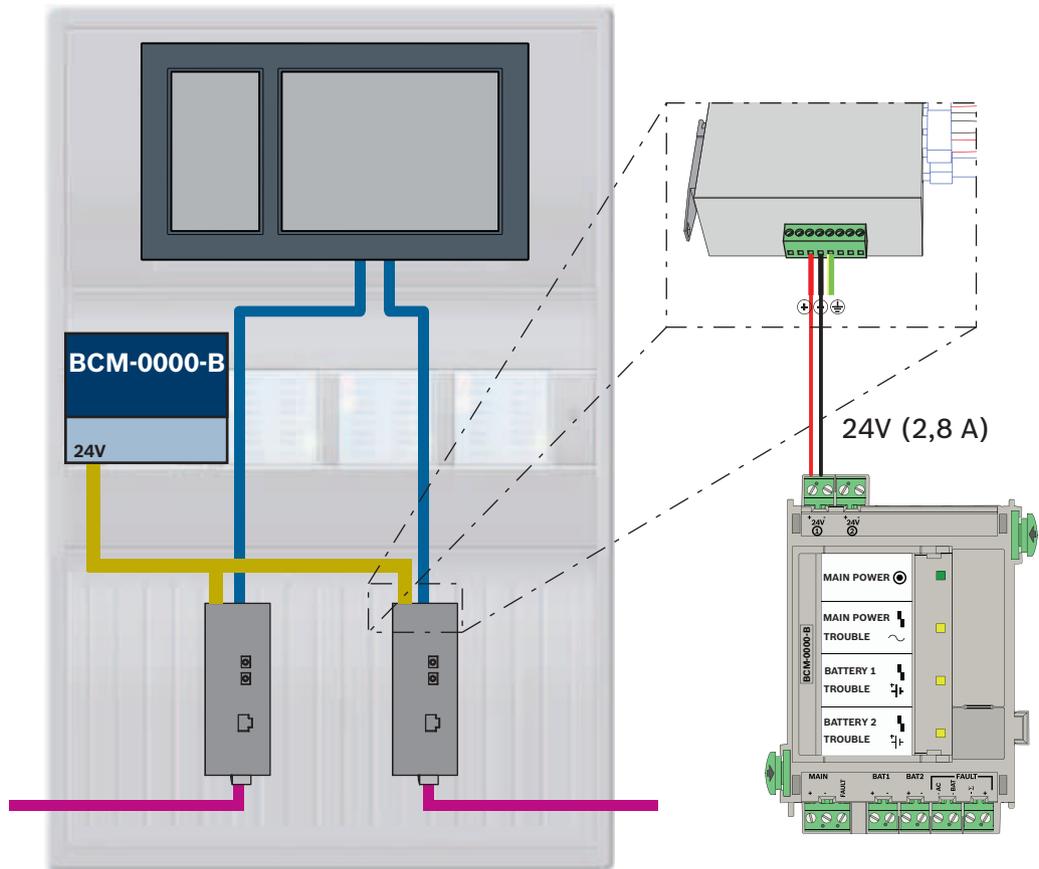
## 11.1 Преобразователь среды

### Подключение преобразователей среды



**Замечание!**

При подключении кабелей FX преобразователей среды отметьте направление передачи по опволоконным кабелям.



**Рис. 11.1:** Подключение преобразователя среды к источнику питания и к входу IN1/IN2 контроллера панели

Значок	Описание
	Кабель Ethernet TX (медный)

Значок	Описание
	Кабель Ethernet FX (оптоволоконный)
	Питание 24 В
	Передача неисправности
	Преобразователь среды

## 11.2 Коммутатор Ethernet

### Подключение коммутатора

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

### Замечание!

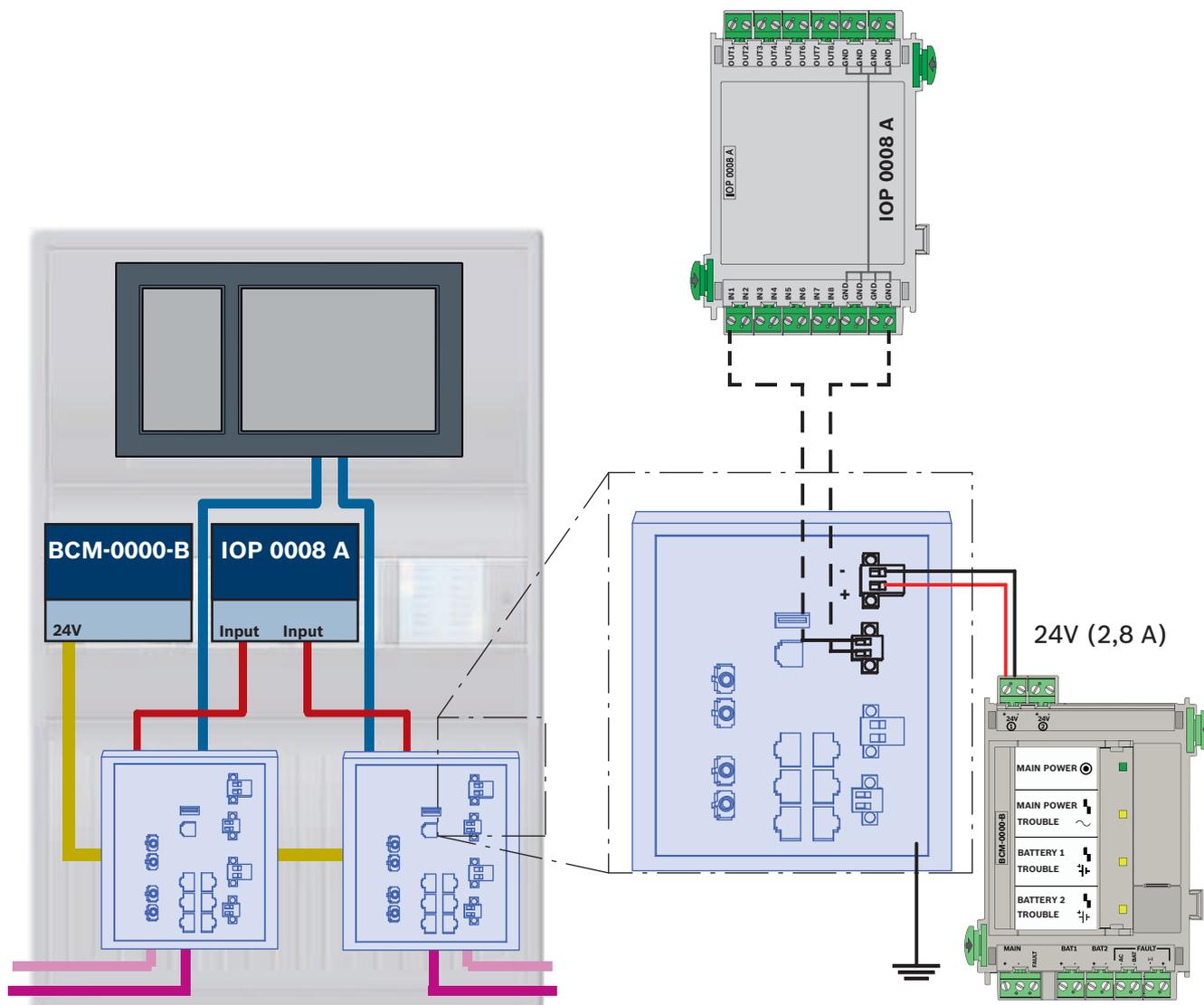


Реле неисправности требуется подключать только для приложений, для которых выполняется хотя бы одно из следующих требований:

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

Источник питания переключателя предусматривает резервирование.

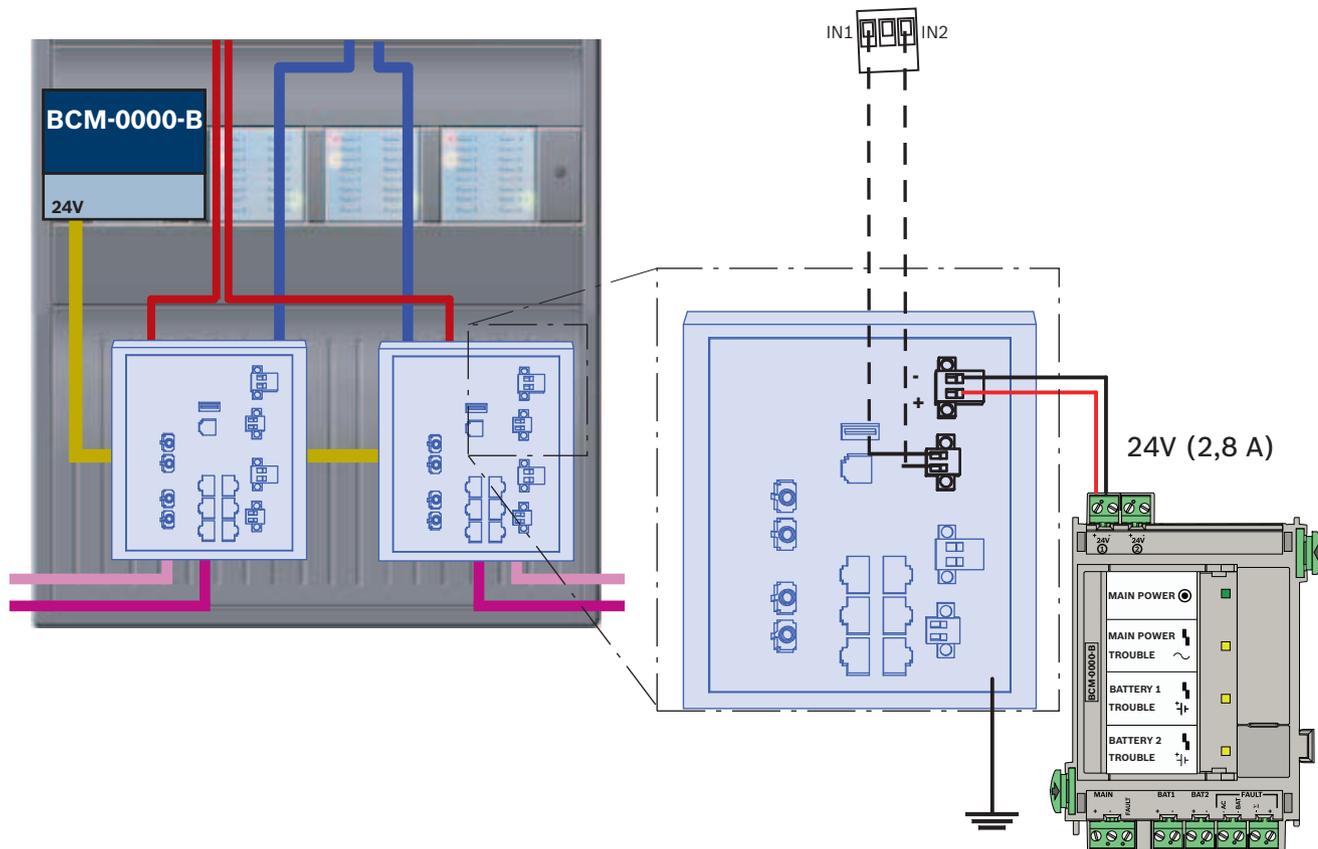
**Подключение коммутаторов с реле неисправности к входам модуля IOP:**



**Рис. 11.2:** Подключение коммутатора к источнику питания и IOP

Значок	Описание
	Кабель Ethernet TX (медный)
	Кабель Ethernet FX (оптоволоконный)
	Питание 24 В
	Передача неисправности
	RSTP-коммутатор

**Подключение коммутаторов с реле неисправности к входам контроллера панели**



**Рис. 11.3:** Подключение коммутатора к источнику питания и контроллеру панели

Значок	Описание
	Кабель Ethernet TX (медный)
	Кабель Ethernet FX (оптоволоконный)
	Питание 24 В
	Передача неисправности
	RSTP-коммутатор



**Замечание!**

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

## 11.3 Удаленная клавиатура

Питание к удаленной клавиатуре должно поступать через внешний источник питания FPP-5000. Подключение к сети устанавливается через 2 медиаконвертера в PSS 0002 A или USF 0000 A.

**Замечание!**

Обратите внимание, что внешний источник питания FPP-5000 и PSF 0002 A (PSS 0002 A) должны быть установлены в непосредственной близости (без промежуточного пространства) от удаленной клавиатуры. Должна быть исключена возможность касания соединительных кабелей между компонентами, поскольку не осуществляется контроль опасности их обрыва и короткого замыкания.

**Замечание!**

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

**Замечание!**

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

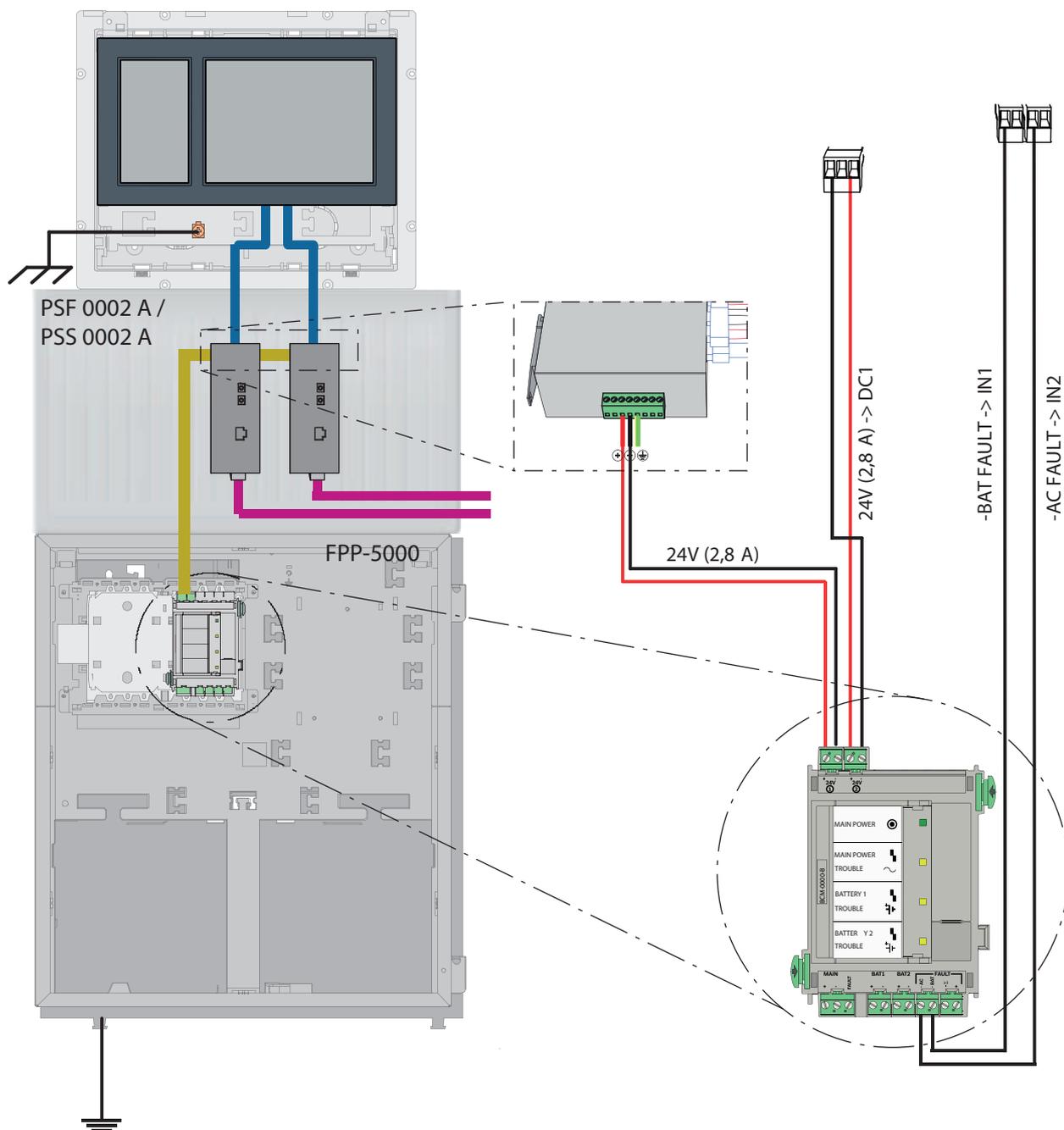


Рис. 11.4: Кабельная сеть удаленной клавиатуры

Значок	Описание
	Кабель Ethernet TX (медный)
	Кабель Ethernet FX (оптоволоконный)
	Источник питания 24 В
	Преобразователь среды

## 12 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.

### 12.1 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 адрес 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 OPC-сервер, систему Praesideo/PAVIRO, сервер UGM-2040 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.

### 12.2 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 как в окне необходимо задать номер 0 для всех подключений.

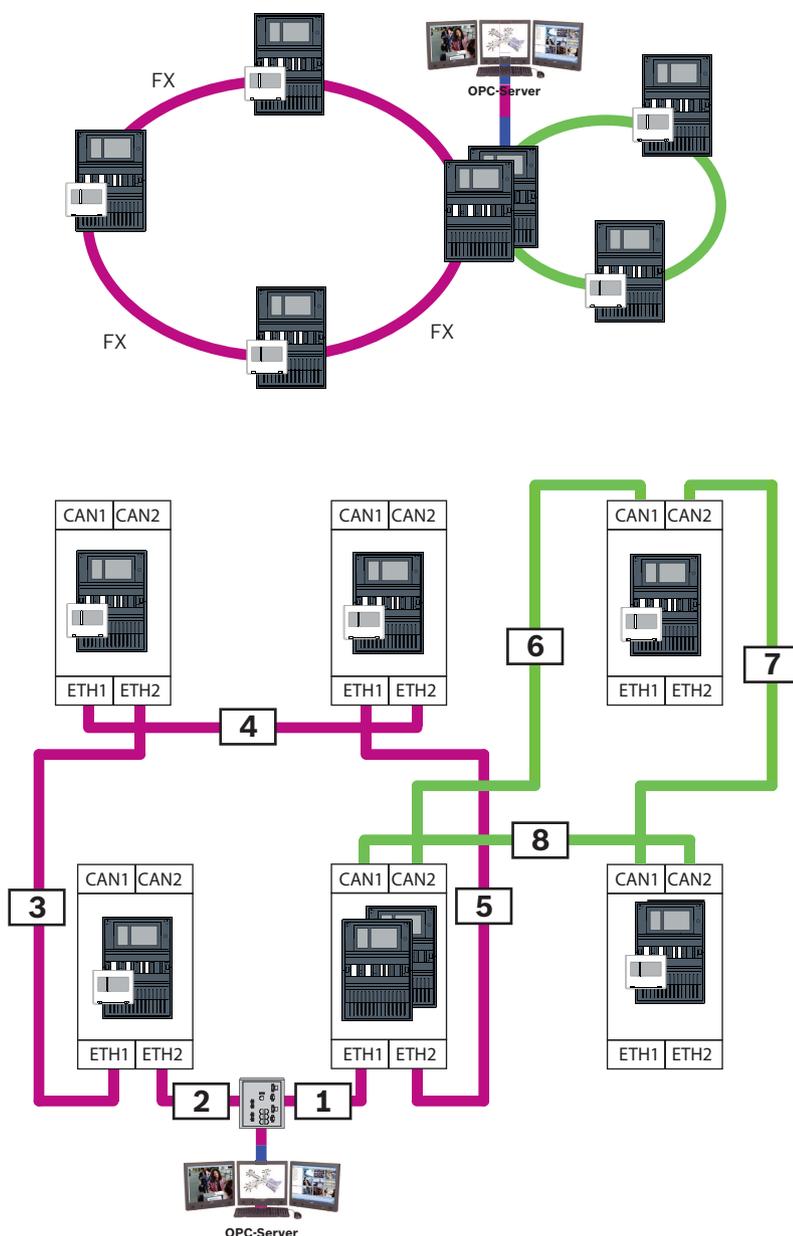


Рис. 12.1: Пример сети и возможной нумерации линий

## 12.3

### 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.

## 12.4

### OPC-серверы

OPC-серверы в вашей сети должны быть добавлены в ПО конфигурирования FSP-5000-RPS.

В программном обеспечении FSP-5000-RPS и на OPC-сервере необходимо выполнить следующие настройки:

- Сетевые узлы
- Сетевая группа
- RSN

- IP-адрес
  - Порт
- По умолчанию OPC-сервер использует порт 25000.

**Замечание!**

EN 54



Подключение к системе управления зданием (например, BIS) через интерфейс Ethernet и OPC-сервер или FSI-сервер совместимо с EN54, только если функции EN54 выполняются исключительно пожарной панелью. Любые связанное с EN54 управление или администрирование (например, управление оповещателями или администрирование отключения) системы управления зданием требует индивидуальной EN54-сертификации всей системы органом сертификации.

**Замечание!**

Программа конфигурирования FSP-5000-RPS

Необходимо назначить OPC-сервер всем сетевым узлам, с которых требуется передавать статусы.



## 12.5

### Серверы UGM-2040

**Замечание!**

Все контроллеры панели и серверы UGM 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.

**Замечание!**

Необходимо назначить сервер UGM-2040 всем сетевым узлам, с которых требуется передавать статусы.



Чтобы подключить панель к UGM-2040, в RPS необходимо смоделировать физическую структуру сети. Сюда также входят номера линий между соединяющим контроллером панели и коммутаторами UGM-2040.

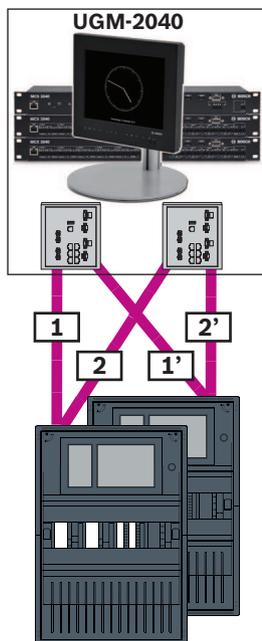


Рис. 12.2: Пример нумерации строк для UGM-2040

## 13 Приложение

### 13.1 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		Имеется несовместимая версия ПО сети панелей. Существует 2 разные версии программного обеспечения.
Групповые ошибки, связанные с сетью			
135.0.6.1	Сеть 2.1		IP-адрес назначен дважды.
135.0.6.2	Сеть 2.2		Конфигурация IP указанной в отчете панели отличается от конфигурации RPS
135.0.6.3	Сеть 2.3		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		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		Изменилась топология сети RSTP. Например, в сеть добавлено другое RSTP-устройство. Это сообщение также может появляться в случае прерывания в линии.

Физ. адрес	Логич. адрес	Сообщение об ошибке	Описание и возможная причина
135.0.7.3	Сеть 3.3		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		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		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		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		Передача данных в линию Ethernet 2 ограничена. Возможные причины включают: разрыв кабеля, кабель не подключен, помехи в кабеле.

## Указатель

### Символы

Адрес физического узла	13
Адресация	
Адрес физического узла	13
Диаметр сети	22
Защищенный сетевой шлюз	35, 40
Интерфейс CAN	12, 49
Интерфейс Ethernet	49
Интерфейс RS232	49
Интерфейс USB	49
Контроллер панели	
Подключение	49
Максимальные ограничения	12
Ограничения: сеть	12
Параметры	
RSTP	14
Параметры RSTP	14
Резервирование	
Адресация	13
Сетевое подключение через CAN	8
Сетевое подключение через TCP/IP	8
Сеть	
Адресация	52
Длина кабеля	26
Кабель	27
Кольцевая топология	26
Ограничения	12
Сеть CAN	8
Сеть Ethernet	8
Сеть: проводка	27
Сеть: разводка	27
Сеть:Контроллер панели	49
Система речевого аварийного оповещения	43
Система речевого оповещения	42
Службы Remote Services	35, 40
Подключение защищенного сетевого шлюза	40
Разделение подсетей	41
Создание учетной записи для Remote Portal	40
Установка удаленного подключения	42
Стандартные настройки, Ethernet	14
Топологии CAN	11
Топологии Ethernet	11
Топологии, CAN	11
Топологии, Ethernet	11
Услуги	8
<b>Е</b>	
Ethernet, стандартные настройки	14

### L

LLDP	22
------	----

### M

MAC-адрес	21
-----------	----

### O

OPC-сервер	8, 49
------------	-------

### P

PAVIRO	8, 42, 43
Praesideo	8, 42, 43

### R

Remote Alert	37
Remote Connect	35
Remote Maintenance	38
для Private Secure Network	38
для Remote Portal	38
Remote Portal	38, 40
Remote Services	
Лицензия	42
Назначение лицензии	42
Перезаказ лицензии	42
RSN	13
RSTP	22









**Bosch Sicherheitssysteme GmbH**

Robert-Bosch-Ring 5

85630 Grasbrunn

Germany

**[www.boschsecurity.com](http://www.boschsecurity.com)**

© Bosch Sicherheitssysteme GmbH, 2020