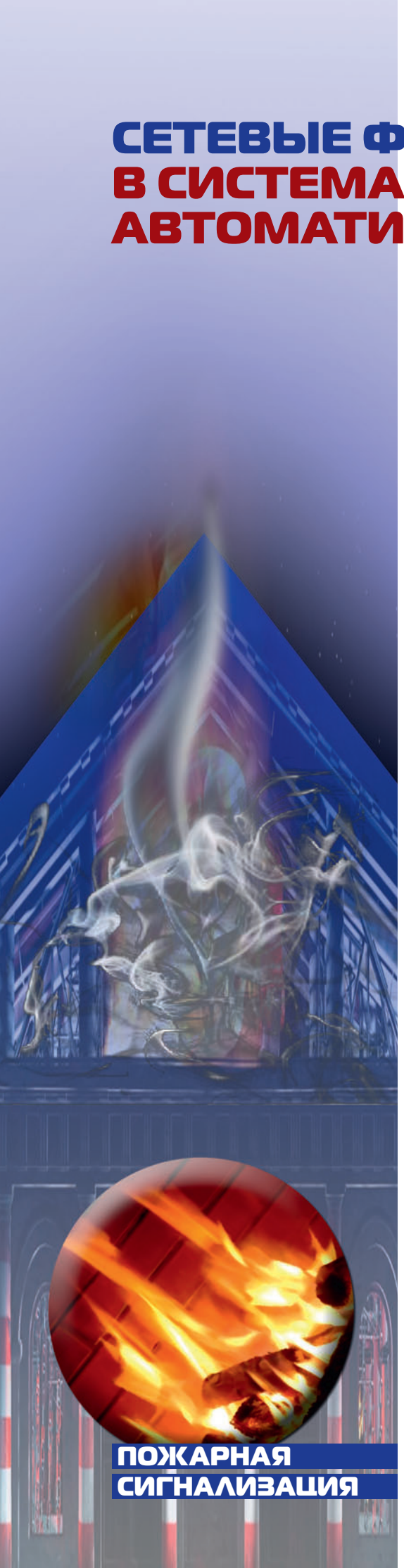
СЕТЕВЫЕ ФУНКЦИИ В СИСТЕМАХ ПОЖАРНОЙ АВТОМАТИКИ

Зайцев Александр Вадимович
научный редактор журнала «Алгоритм безопасности»



Не все специалисты сразу смогут понять, зачем вообще появилась необходимость поднимать этот вопрос сейчас. Похоже на какую-то экзотику. Кажется, что это не та проблема: проложили между компонентами приемно-контрольного прибора (ППКП) шину RS-485 и связали по ней столько блоков и модулей, сколько душа позволит. Таким образом можно получить у одного ППКП практически ничем не ограниченную информационную емкость, хоть на 100000 пожарных извещателей (ИП). И по сигналам от этих ИП запустить такое же неограниченное число исполнительных устройств пожарной автоматики (ПА). Так делали, делают и менять ничего не собираются.
Только вот наступает время для исключения в системах пожарной сигнализации (СПС) подобного безобразия. Во всем мире о таких вариантах уже давно забыли. Этому и будет посвящена данная статья.

ОПЯТЬ ПРО УСТОЙЧИВОСТЬ СПС

В соответствии с техническим регламентом Евразийского экономического союза «О требованиях к средствам обеспечения пожарной безопасности и пожаротушения» ТР ЕАЭС 043/2017 [1] в настоящий момент проводятся работы по разработке межгосударственного стандарта «Приборы приемно-контрольные пожарные. Приборы управления пожарные. Общие технические требования. Методы испытаний».

В нем будет очень много принципиально нового, и все это новое уже давным-давно регламентируется в зарубежных директивах по пожарной безопасности. Пора и нам привыкать.

Начну с того, что в зарубежных нормах по системам пожарной сигнализации (СПС) помимо вопроса о возможном отказе при единичном отказе любой линии связи не более 32 автоматических извещателей, стоит еще вопрос о нарушении по этой же причине не более одной функции при срабатывании ручных извещателей, звуковых оповещателей и устройств ввода/вывода. Вплоть до того, что если в автоматическом пожарном извещателе предусмотрен еще и встроенный оповещатель, то в этом корпусе или с двух его сторон в линии, к которой он подключен, должны находиться изоляторы короткого замыкания, как и в ручных пожарных извещателях и модулях ввода/вывода. Это для адресных систем.

Для неадресных систем в любом шлейфе сигнализации не может быть более 32 автоматических пожарных извещателей, а от каждого оповещателя или модуля нужно подводить чуть ли не свою индивидуальную линию связи на отдельный выход или вход прибора. А как быть, если стоят задачи по обеспечению реальной работоспособности систем противопожарной защиты?

Примерно то же самое планируется реализовать и у нас в стране.

Это является следствием необходимости выполнения условий живучести противопожарных систем, которая характеризуется свойством систем сохранять способность выполнять требуемые функции в условиях, создаваемых воздействиями внешних дестабилизирующих факторов.

Одним из главных факторов живучести сетей электросвязи является связность системы. Сетевые методы обеспечения живучести касаются топологии построения систем и обеспечиваются изменением разветвленности и увеличением резервирования линий (каналов) связи в сети с целью увеличения ее показателей связности до требуемых значений.

По крайней мере, кольцевые линии связи являются необходимым, но недостаточным условием доведения коэффициента связности до минимальной величины, обеспечивающей требуемую устойчивость при единичном отказе любой линии связи, и равной 2.

Но есть еще одно, для нас принципиальное, новшество в построении СПС. Это ограничение емкости ППКП.

В пункте 13.7 EN 54-2 «Системы пожарной сигнализации. Часть 2. Приборы приемно-контрольные пожарные» предусмотрено, что если производитель считает возможным к ППКП подключать более 512 пожарных извещателей, как автоматических, так и ручных, то он должен указать мероприятия, которые при системной ошибке в самом ППКП как минимум

исключат по этой причине отказ более чем 512 пожарных извещателей. В таких ППКП резервируется все, что можно и нельзя, и должно быть обеспечено в нем еще и наличие устройства контроля выполнения процессором программы с наличием соответствующей индикации. На это контрольное устройство еще возложена функция по перезапуску программного обеспечения – то, что мы частенько сами делаем на компьютере (заветные клавиши Ctrl+Alt+ Del).

Все это в том или ином виде будет иметь место и в стандарте «Приборы».

РОЛЬ СЕТЕВЫХ РЕШЕНИЙ В ПРОТИВОПОЖАРНОЙ ЗАЩИТЕ ОБЪЕКТОВ

Из предыдущего раздела можно сделать вывод: отказ любой линии связи в электроуправлении системами противопожарной защиты (СПЗ) не должен приводить к отказу более чем 32 автоматических ИП, более одной функции при срабатывании ручных извещателей и устройств ввода/вывода, а также отказ ППКП не должен приводить к отказу более чем 512 автоматических ИП. Для простоты дальнейшего рассмотрения материала данной статьи я предлагаю все эти требования объединить под аббревиатурой «32/512».

Обо всем этом я писал в [2-5].

Я знаком со многими отзывами читателей на представленный материал. Самое мягкое предложение – спуститься с небес, куда меня занесло волею случая, и забыть о своих фантазиях как о страшном сне. Но это было в 2014 году, за прошедшее время в умах моих читателей кое-что, я надеюсь, изменилось.

Так вот, те, кто до сих пор сомневается в моей правоте и целесообразности внедрения в жизнь даже в отдаленной перспективе этих требований, могут открыть проект готовящегося стандарта «Приборы» и найти в нем практически все, о чем я когда-то писал. Безусловно, в процессе дальнейшей работы над стандартом многое что еще изменится, но только не эти принципиальные моменты.

А теперь представьте себе, что только два указанных мною момента, позиционируемые как «32/512», приведут к серьезнейшим изменениям как в самих приборах, так и в практике их применения. И самыми главными техническими решениями станут сетевые решения.

Я уверен, что большинство специалистов уже достаточно наслышаны о поразительных возможностях целого ряда зарубежных производителей, выпускающих мощнейшие системы противопожарной защиты. Такие объекты, как аэропорты международного класса, крупнейшие железнодорожные вокзалы, бизнес-центры (в т. ч. и подобные «Москва-Сити»), крупные магазины (ГУМ в Москве или Гостиный двор в Санкт-Петербурге и т. п.), в принципе не могут обойтись без их оборудования. И как в данном случае можно обойтись без приборов, соединенных между собою сетью, я даже не представляю.

Есть и не такие грандиозные объекты, но перед многими из них стоят не менее сложные задачи, так как их посещают сотни, а то и тысячи людей, безопасность которых должна быть обеспечена. И радиолюбительским решениям от юных Василис тут не место.

Поэтому требования к техническим средствам пожарной безопасности всегда повышались и дальше будут повышаться параллельно с развитием всех современных технологий. В настоящий момент этот импульс развития дают сетевые технологии.

ОСОБЕННОСТИ СЕТЕВЫХ РЕШЕНИЙ В ТЕХНИЧЕСКИХ СРЕДСТВАХ ПА

Если кто-то подумает, что речь пойдет об общеизвестных IT-технологиях, то он глубоко заблуждается. В том виде, как они используются в компьютерных сетях, их не будет, можете не надеяться, данный вариант изначально исключен. Это лишний раз подтверждает международная практика. Помните, как в известной пословице, только с некоторыми изменениями: «То, что кому-то хорошо, для другого смерти подобно». Так и здесь, в системах противопожарной защиты.

Почему и с чем это связано? Будем разбираться в данном разделе.

Если попытаться соединить, как это сейчас принято делать, между собою приборы или их компоненты, разнесенные по всему объекту, по одной общей как радиальной *(рис. 1)*, так и кольцевой шине RS-485 или ей подобной, то любой отказ в этой шине однозначно приведет к отказу в СПС более 32 ИП. В кольцевой шине RS-485 не помогут даже изоляторы короткого замыкания (ИКЗ), в лучшем случае, они смогут отсечь один прибор, на входе которого произошло короткое замыкание (КЗ), что также недопустимо в свете требований «32/512».

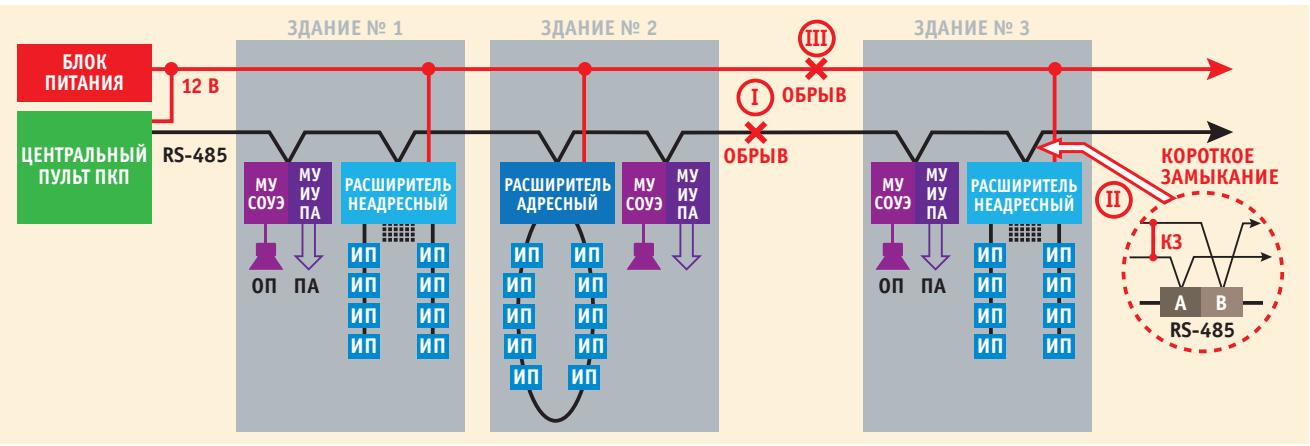
Еще не надо забывать, что в стандарте TIA/EIA-485 «Electrical Characteristics of Generators and Receivers for Use in Balanced Digital Multipoint Systems» для шин по RS-485 эти ИКЗ просто не предусмотрены. Какая-то защита может быть реализована только при использовании, как минимум, двух независимых линий с гальванической развязкой между собою на всех входах и выходах устройств.

Точно такая же ситуация, как с использованием стыка RS-485, будет, если какой-то прибор верхнего уровня соединить самостоятельными линиями связи с приборами нижнего уровня. Отказ любой из них, и опять нарушение требований «32/512».

Вот уже три типовых топологических структуры оказались не пригодными для реализации. Добавим к ним в качестве четвертой еще древовидные IT-сети. Отказал один ее узел, и на всей системе можно поставить крест.

Вроде бы альтернативой могут быть кольцевые IT-структуры с использованием современных маршрутизаторов. Когда-то, чуть более 10 лет назад, для меня

Рис. 1. Существующая топология построения системы противопожарной защиты на базе стыка RS-485



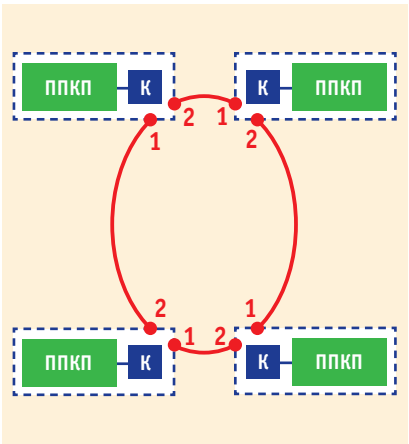
это стало находкой, и я ей несказанно обрадовался и даже имел удовольствие использовать. Действительно, в этих структурах можно гарантировать обмен данными между всеми устройствами при единичных отказах линий связи между маршрутизаторами. Осталось только до минимума уменьшить расстояние между прибором и самим маршрутизатором, поставить между ними преобразователь RS-485 в Ethernet, и цель достигнута. Но не тут-то было, и это я понял, к сожалению, чуть позже.

Несмотря на то, что маршрутизаторы сами могут без чьего-то вмешательства выполнять серверные функции по обмену данными в сети, как по основным, так и по резервным маршрутам, за состоянием этой сети нужен еще внешний контроль. Кто-то, в конце концов, должен же как-то узнавать, что весь резерв маршрутов исчерпан. Как правило, для этого используется сервер мониторинга, находящийся в каком-нибудь компьютере, подключенном к одному из маршрутизаторов сети, который будет выводить на свой экран состояние этой сети.

А про отрицательное отношение к компьютерам в противопожарных системах всем хорошо известно, поэтому и не буду здесь останавливаться.

Но появляется еще одно препятствие в использовании стандартных маршрутизаторов и компьютеров ввиду необходимости обеспечения бесперебойного питания по пожарным нормам. А это, надо отметить, тоже не тривиальная задача, многие специалисты уже наверняка с этим сталкивались и пытались героически преодолеть возникшие на их пути трудности. В зависимости от количества и типов портов у маршрутизатора емкость резервной батареи может находиться от 14 до 40 А/ч, а тут и вовсе можно оказаться без требуемого пожарного сертификата на источник бесперебойного питания. Поэтому с пожарными сертификатами и у маршрутизаторов не все в порядке, и неспроста.

Рис. 2. Цепочечно-кольцевая структура



Так уж повелось, что в системах ПА за контроль целостности линий связи отвечает какой-нибудь прибор, к которому они подключены, это одна из прямых его задач. В сетях из пожарных приборов за непрерывный контроль должен отвечать и выдавать информацию об их состоянии хоть один из приборов любой такой сети. И как же с компьютера, обеспечивающего контроль состояния сети, всю необходимую информацию запихать в этот прибор?

Самое простое, конечно, все без исключения оборудование разместить в одном месте или даже сгруппировать в каких-то технологических шкафах.

Релейные выходы одних приборов соединить с входами других, и наоборот, для организации межприборных связей, ввиду недостаточной информационной емкости каждого из них по отдельности.

Но тогда придется столкнуться с проблемой длинных неадресных шлейфов и линий связи к исполнительным устройствам пожарной автоматики, что тоже не очень хорошо, и, по большей части, влечет за собой другие большие и даже очень большие проблемы.

Кстати, это все это является причиной того, что импортные пожарные приборы, как правило, выполняются в моноблочном исполнении, произвольно размещаются на объекте поближе к местам выполнения своих функций и соединяются уже между собою с помощью сети. Так намного надежнее, проще и дешевле, чем думать, как соединить между собою массу удаленных блоков и модулей.

Вот мы и пришли к тому, что в пожарных приборах, в соответствии с новыми требованиями, может или должна появиться новая функция – работа в сети одно/или разнотипных приборов и их компонентов.

Оглянитесь теперь назад, и посмотрите, какой путь для понимания этого вопроса понадобилось пройти, но дальше все уже будет намного проще.

ПРАКТИЧЕСКИЕ ВОПРОСЫ СЕТЕВЫХ РЕШЕНИЙ В ПА

По поводу требований к реализации сетевых решений в СПС в зарубежных нормах практически ничего нет. Пожалуйста, стройте свою СПС, как вам захочется, только обеспечьте выполнение требований по части «32/512» и необходимую индикацию как отказавших устройств в сети, так и линий связи между ними. Потому что у них эти требования по устойчивости предъявляются не столько к приборам, сколько ко всей СПС, а уж как ее с учетом этих требований построить – ваше дело.

Как правило, устройства связи в сети, а их еще очень часто называют коммуникаторами или модулями связи, являются опцией для любого импортного ППКП средней и большой информационной емкости. Т. е. этот коммуникатор может как присутствовать в комплекте ППКП, так и отсутствовать.

У коммуникатора предусматривается, как минимум, два порта для работы в сети и один порт для взаимодействия со своим прибором. Для этого в корпусе прибора или в стоечном монтаже может выделяться место для его установки.

К самому коммуникатору, помимо всего прочего, предъявляется требование, чтобы или его отказ, или отказ в линиях связи, к которым он подключен, не влияли на работу самого ППКП. И наоборот, чтобы отказ в ППКП ни в коем случае не влиял на работу коммуникатора в сети, иначе не будет выполнено требование «32/512».

Некоторые производители на коммуникаторы возлагают еще одну из функций по резервированию основного процессора прибора. При отказе процессора, по команде от устройства контроля за работой программного обеспечения прибора, коммуникатор напрямую подключается к контроллеру адресного шлейфа своего прибора и передает на один из других, заранее определенных приборов всю информацию, поступающую от контроллеров адресного шлейфа. Вот какими умными бывают пожарные приборы.

В сети между собою коммуникаторы, как правило, за некоторым исключением, соединяются по цепочечно-кольцевой структуре, от одного к другому, как показано на *рисунке 2*, на котором коммуникаторы обозначены буквой К. В этом случае отказ любой линии связи между коммуникаторами приведет только к переходу от кольцевой замкнутой структуры к радиальной, без потери какого-либо прибора этой сети.

Гораздо реже используется две радиальные линии, прокладываемые по разным трассам. Но сами эти линии и порты, к которым они подключаются, должны функционировать абсолютно независимо друг от друга.

Выпускаются коммуникаторы как для работы по проводным линиям связи, так и по ВОЛС. Существуют коммуникаторы на 4 и более линий связи. В этом случае с их помощью возможно построение кольцевых линий разного уровня. К примеру, внутри отдельного блока здания прокладываются кольца с несколькими приборами по проводным линиям, а для объединения этих колец между собою – кольцевые линии верхнего уровня на оптоволокне, что приведено на *рисунках 3 и 4*.

В одноуровневой сетевой структуре из 5 кольцевых линий, представленной на *рисунке 3*, связность в основном равна 2, но есть в ней слабые звенья в виде 4 коммуникаторов, находящихся на объединяющем кольце.

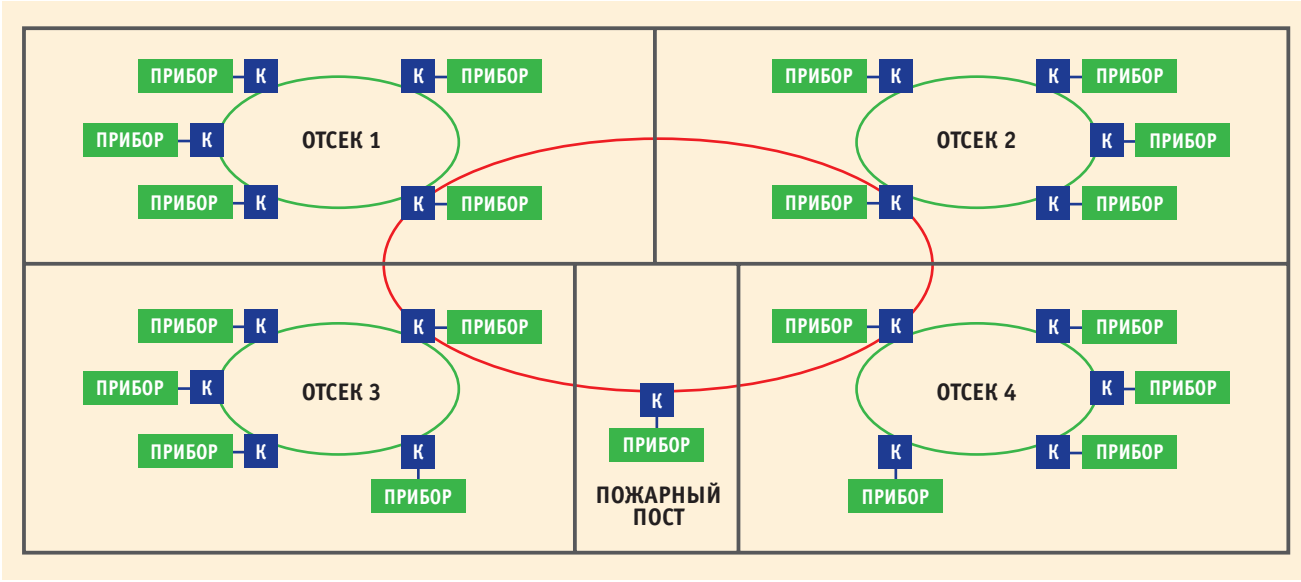


Рис. 3. Одноуровневая сетевая структура СПС

Двухуровневая структура, также из 5 кольцевых линий, представленная на *рисунке 4*, свободна от указанных недостатков и связность в ней выше 2.

ЗАДАЧИ В СЕТЯХ ИЗ ПОЖАРНЫХ ПРИБОРОВ

Я много раз слышал предложения наших отечественных проектировщиков о введении в России единого стандарта по обмену данными в шлейфах адресных систем ПС. Мол, у одного производителя хороший и недорогой прибор, а другого достаточно приличные и недорогие адресные пожарные извещатели. Вот и заставим их работать по единому протоколу, чтобы у нас был маневр. Это утопия.

Но, переходя к сетям, я уверен, тема не закрыта: заставить производителей обеспечить единый протокол обмена и в сетевых решениях, да так, чтобы в одной сети можно было использовать разные типы оборудования абсолютно разных производителей.

Это еще большая утопия. Такая универсальность ничего не даст кроме непредсказуемых проблем. И как быть в этом случае с импортным оборудованием?

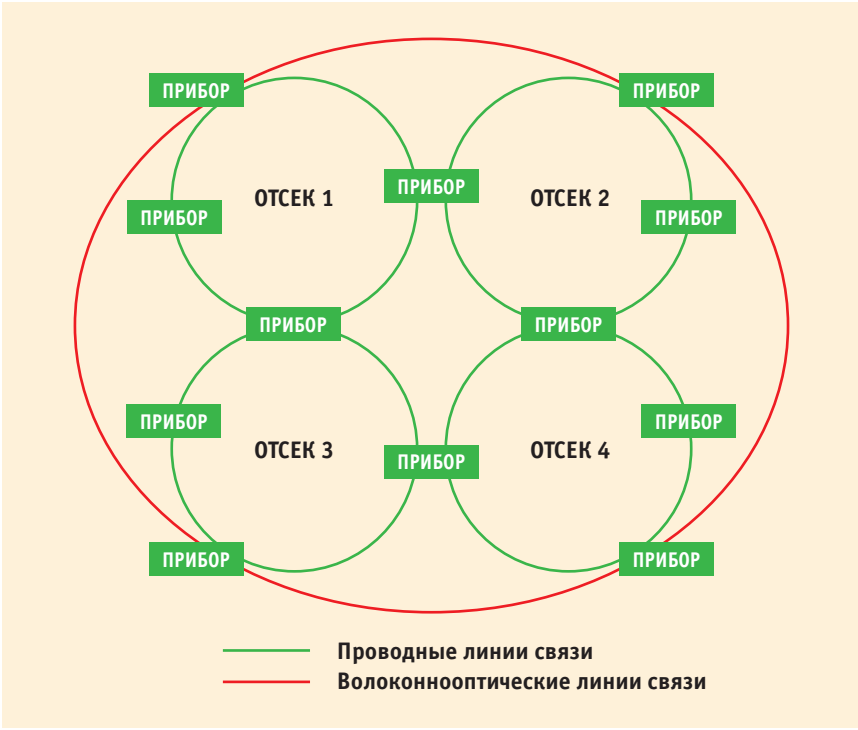
Поэтому каждый зарубежный производитель разрабатывает свои протоколы обмена в сети. В подавляющем большинстве они базируются на транспортном протоколе Ethernet, но формат кадра данных у каждого свой. Отсюда и появляются essernet, SecuriLan, Integral LAN, SAFEDLINK и множество других.

В качестве примеров коммуникаторов можно привести:

1. Контроллеры связи FX-MC2 (FX-SAA, FX-SAB или FX-SAC) систем пожарной сигнализации FX 3NET (Schneider Electric Buildings Business), рассчитанные на работу по двум параллельным проводным линиям по стандарту RS-485.
2. Сетевой блок B6-NET2-FX (S/M) для подключения до 16 панелей управления серии SCP2000, SCP3000 системы SecuriFire (Securiton) в кольцевые линии сети посредством оптоволоконного кабеля.
3. Модули 784840.10/784841.10 для сети из 16/31 станций IQContol C/M и серии 8000 (Honeywell Life Safety Austria GmbH – Esser) для работы на скоростях 62,5/500 кБит/с соответственно.
4. Модуль интерфейсный оптический одномодовый B5-NET2-FXS, предназначенный для объединения станций Integral IP («Шрак Секонет АГ») в трехуровневую сеть Integral LAN, в которую может входить до 4000 станций. У этого модуля предусмотрены интерфейсы почти на все случаи жизни:

– 4 порта по RS-485со скоростью 1,2 Мбит/с на расстояние до 1200 м;
– 2 порта по Ethernet 100 Base TX со скоростью работы 100 Мбит/с на расстояние до 100 м;
– 2 оптических порта по Ethernet 100 Base FXS для работы на скоростях 100 Мбит/с на расстояние до 10 км.

Рис. 4. Двухуровневая сетевая структура СПС



Уже из приведенного перечня видно, что чем больше приборов в сети, тем выше скорость обмена данными между ними. С другой стороны, известно, что чем выше скорость обмена данными по проводным линиям, тем меньше расстояние между узлами. Поэтому в технической документации производителей все эти моменты должны быть озвучены.

Возможно использование двух вариантов коммуникаторов. В первом – один из них является главным или ведущим, а все остальные подчиненные. Во втором варианте, а он как раз в основном и используется на практике, все коммуникаторы равноправные.

В случае использования равноправных коммуникаторов – каждый из них может транслировать в свой ППКП абсолютно всю информацию из сети и обратно. Остается определить, на каком приборе она нужна, а на каком нет.

Коммуникаторы могут использоваться не только для обмена данными о состоянии технических средств пожарной автоматики, но и для организации распределенной системы оповещения о пожаре и эвакуации людей (СОУЭ), передающей речевые сигналы в цифровом виде без каких-либо искажений на большие расстояния для дальнейшей их подачи на соответствующие усилители мощности.

Для примера здесь можно привести сеть из приборов для СОУЭ «Praesideo» (Bosch), в которой помимо 32 каналов данных для контроля и управления всем оборудованием обеспечивается одновременная передача до 16 аудиоканалов. Еще надо иметь в виду, что большинство устройств системы «Praesideo» для максимальной защиты от наведенных э.д.с. имеют пластиковые оптоволоконные интерфейсы. Пластиковое оптоволокно используется для соединения узлов и блоков, расположенных на расстоянии до 50 м. Для соединения узлов и блоков, расположенных на расстоянии более 50 м, используется более дорогой многомодовый или одномодовый оптоволоконный кабель, в комплекте оборудования предусмотрены соответствующие переходники. Безусловно, такой коммуникатор уже просто так, в виде «дополнительной платки», ни в какой блок не засунешь, и он выполняется как самостоятельное устройство для установки в 19" стойках или шкафах.

Вот вроде и все, что касается коммуникаторов.

НОВЫЕ ФУНКЦИИ В ПРИБОРАХ

Построив с помощью коммуникаторов сеть, мы смогли с ее помощью объединить между собою приборы для их совместной работы.

Что подразумевается под совместной работой?

Возьмем для начала сеть из нескольких ППКП, расположенных в одном здании.

Первое, что нам нужно получить на ППКП, расположенном на пожарном посту, это информацию о всех тревогах и неисправностях со всех ППКП сети. Таким образом, ППКП должен иметь возможность выводить на индикацию не только собственные события, но и все события других, соединенных с ним приборов. А это уже вопросы к индикации. В обратном направлении должны проходить команды на отключения или сброс.

А если это не просто ППКП, а еще и с функцией управления, т. е. ППКиУП, и технические средства оповещения подключены непосредственно к своим приборам, то извещение о пожаре из одного прибора должно запустить оповещение в других приборах.

Точно так же должно происходить и с другими подсистемами ПА: событие в одном приборе должно формировать команды для других приборов.

А как быть с ручным, т. е. дистанционным управлением устройств пожарной автоматики, подключенной к разным приборам? И это тоже необходимо учесть.

А что будет, если эти ППКиУП еще выполняют функции управления противодымной защитой? Вот здесь придется столкнуться с необходимостью написания сложных алгоритмов для каждого прибора в зависимости от наличия тех или иных реакций в системе и подключенного к нему оборудованию. Более того, еще надо понимать, что никакого старшего или главного прибора в сети нет и не может быть, иначе его отказ опять-таки сможет привести к нарушению требований «32/512». Т. е. все приборы в сети равноправны и обязаны в полном объеме выполнять свои задачи на контролируемой ими площади, как если бы они находились в автономном режиме.

В сетях пожарных приборов можно встретить еще такие варианты, как «видящий» и «видимый» приборы. Для «видящих» может определяться список приборов, данные от которых можно просмотреть на этом конкретном «видящем» приборе, и с него предусматривается управление «видимыми». Такая функция позволяет разграничивать доступ персонала к различным группам приборов, находящимся в одной сети. Данная функция может использоваться в зданиях, где имеются разные собственники или арендаторы.

И в завершении темы об особенностях приборов, работающих в сетях, надо упомянуть о необходимости отражать состояние линий связи между самим приборами. В IT-сетях для этого используют компьютер, но его практически невозможно применить в сетях пожарных приборов.

Одной обобщенной индикации здесь недостаточно, она должна идти с указанием между какими приборами или на каком участке сети произошел отказ.

Но не надо забывать, что каждый коммуникатор имеет свои характеристики и совместно с прибором, в котором он установлен; и они не могут обеспечить работу в сети из бесконечного множества приборов. Все определяется возможностями как самого прибора, так и коммуникатора.

Для обнаружения отказов в сети нужно какое-то время, так же как для выявления отказавшего участка, но время необходимо и для восстановления нормальной работы сети с учетом отказавшего участка.

Значит, и в технической документации на них должны быть приведены какие-то конкретные характеристики, а задача стандарта – определить их предельные параметры и методики проверки.

Вот сколько новых функций должно появиться в приборах. А начиналось все лишь с обеспечения устойчивости систем к единичному отказу линий связи.

ЗАКЛЮЧЕНИЕ

В настоящее время идет работа над формированием принципиально новых требований к приборам. Если какие-то моменты уже и рассматривались, и даже использовались на практике, то с сетевыми функциями в системах пожарной автоматики сталкивались только те, кто имел большой опыт работы с импортным оборудованием. Но в обозримом будущем с этим придется иметь дело большинству специалистов проектно-монтажных подразделений. А нашим отечественным производителям в пору уже начать думать, как эти решения реализовать.

ЛИТЕРАТУРА

1. *Зайцев А. В. От федерального закона № 123-ФЗ к техническому регламенту ЕАСС // Алгоритм безопасности. 2018. № 1.*
2. *Зайцев А. В. Живучесть систем противопожарной защиты. Части 1-3 // Алгоритм безопасности. 2014. №№ 4-6.*
3. *Зайцев А. В. Некоторые частные вопросы живучести СПС. Зоны пожарной сигнализации // Алгоритм безопасности. 2015. № 3.*
4. *Зайцев А. В. Система нормирования устойчивости СПС к дестабилизирующим факторам // Алгоритм безопасности. 2016. № 1.*
5. *Зайцев А. В. Нормирование устойчивости АУПС И СПС // Алгоритм безопасности. 2016. № 3.*