Особенности интеграции приемно-контрольных приборов в единую сеть

Сергей ЛЁВИН,
главный конструктор научно-производственной фирмы «Сигма – Интегрированные Системы»

При построении системы безопасности (СБ) зачастую не удается свести все емкость системы на одну «голову». Хотя, конечно, есть приборы большой емкости (до 1000 шлейфов сигнализации и даже больше). Но ведь всё равно существует ограничение информационной емкости одного прибора. К тому же, иногда невозможно завести на один прибор все извещатели и другие источники информации из-за территориальной распределенности объекта охраны, его развития и, соответственно, наращивания СБ. А уж когда независимо проектируются и затем монтируются различные подсистемы, часто – разными организациями, СБ почти неизбежно «разваливается» на несколько независимых частей. А задачу эти части должны решать общую, и, скорее всего, без какой-либо интеграции, то есть налаживания совместной работы путем обмена полезной информацией, сделать это на должном уровне нельзя.

Интеграция между подсистемами ОПС решает следующие задачи:
- вывод информации со всех приборов на один;
- в пожарной сигнализации – выдача сигнала «Пожар» другим приборам для совместного управления оповещением и инженерными системами (вентиляция, дымоудаление, лифты и т.п.);
- в охранной сигнализации – возможность управлять одним прибором через другой (постановку на охрану зоны второго прибора с терминала, подключенного к первому).

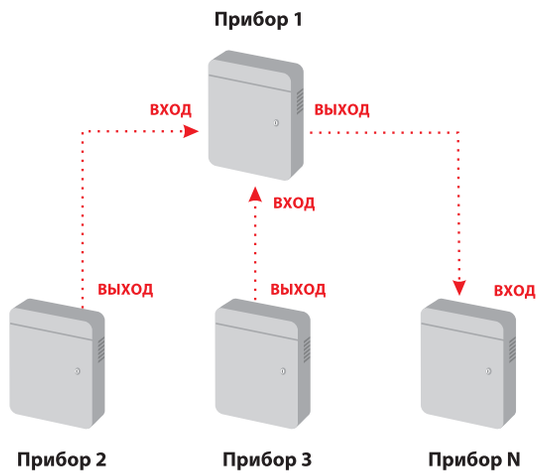
Назову также несколько вариантов интеграции между различными подсистемами:
- пожарная сигнализация и СКУД: разблокировка дверей при пожаре
- охранная сигнализация и СКУД: блокирование дверей при тревоге
- охранная сигнализация и СКУД: использование терминалов СКУД (считывателей) для управления процессом объектовой постановки на охрану / снятием с охраны
- блокирование точек доступа в помещения, поставленные на охрану.

Способы интеграции хорошо известны специалистам: программная, – через ПО верхнего уровня, - и аппаратная интеграция, - когда приборы «договариваются» между собой сами, не используя программный верхний уровень.

Использование интегрирующего ПО обеспечивает совместную работу разного оборудования. ПО позволяет создать единое информационное пространство и прозрачность при работе с системой, в состав которой входит несколько приборов.

Если же говорить об аппаратной интеграции, то в простейшем случае совместная работа приборов может осуществляться через «сухие контакты». Выход одного прибора подключается к входу другого, и все, связь налажена. Минусом такого способа является низкая информативность – по одному подключению можно передать только одно извещение.

Объединение приборов через "сухие контакты"

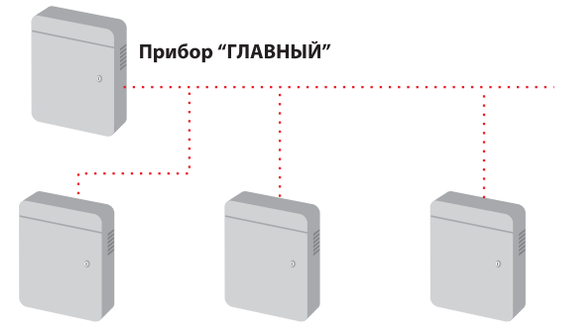


Гораздо более эффективным способом является объединение приборов в сеть по какому-либо цифровому интерфейсу.

Если на объекте используется оборудование разных производителей, то говорить об интеллектуальной аппаратной интеграции практически не приходится. Как правило, все фирменные протоколы закрыты и являются оригинальными. Выход - использовать открытые технологии и протоколы, например, Lonworks. Это делают многие компании, и у ведущих производителей имеются в линейке продуктов специальные устройства, которые, по сути, являются шлюзами в LON-сеть. Довольно широко распространена сегодня и технология BACnet, которая уже имеет стандартизованные профили устройств для систем безопасности, рекомендуемые ассоциацией BACnet как стандартные. В них уже есть расширения по системам безопасности – точка доступа, датчик, связанный с охранно-пожарной сигнализацией. С помощью таких глобальных технологий можно реализовывать аппаратную интеграцию. Но чаще стоит более простая задача – оборудование одного производителя увязать аппаратно вместе. Простой пример: оператору удобно работать, когда сообщения с нескольких приборов приходят на один. Перед ним находится не десять терминалов и десять дисплеев, а всего лишь один монитор, на который выводится вся информация о системе. По сути дела это – централизация выдачи сообщений.

Следующий вопрос – взаимодействие подсистем. Способов аппаратной интеграции достаточно много, и самый простой и надёжный – это уже упомянутые «сухие контакты». Надежность этого способа близка к абсолютной. Не случайно сегодня это очень широко используется. Например, для обеспечения связи между пожарной сигнализацией и системой контроля доступа, – там до-

Объединение приборов в сеть Master-Slave



статочно групповых сигналов, большой информативности не нужно, поэтому можно общий сигнал с пожарной сигнализации передать в систему контроля доступа. А на большом объекте можно применить зонирование. Совсем другое дело, когда пытаются передать таким способом сотни сигналов, тогда это всё превращается в бухты кабелей.

Интеллектуальное объединение приборов – это когда приборы объединяются в так называемую сеть. Очень популярно объединение посредством последовательных шин. Самое применяемое – RS-485. Это – промышленный интерфейс, который, собственно, для этого и предназначен. Разработано огромное количество протоколов, как фирменных, так и открытых, реализованных на интерфейсе RS-485. Протоколы эти в подавляющем большинстве работают по принципу Master - Slave (главный – подчиненный). У подобного подхода есть свои преимущества и недостатки. Основной недостаток этого способа объединения состоит в том, что выбирают «главенствующий» прибор, с помощью которого организуют взаимодействие, сбор информации, передачу данных. И именно один, как я уже сказал, «главенствующий» прибор определяет работоспособность всей системы. Соответственно, при выходе из строя этого прибора сеть просто перестанет работать.

Более устойчива система, в которой используются только одноранговые (равноправные) приборы. В ней не выделяется какой-то главный. В качестве «транспорта» для такой сети наиболее часто используется тот же Ethernet, и это сейчас очень доступно, на любом объекте можно организовать локальную сеть. Причём, это может быть локальная сеть всего предприятия или обслуживающая исключительно системы безопасности. В этом случае при инсталляции и конфигурировании системы определяются связи и правила взаимодействия оборудования. Система при таком построении намного надёжнее, потому что выход из строя линии связи между приборами или одного из приборов не должен никак отражаться на совместной работе других приборов с ненарушенной связью. На важных объектах применяют и дублирование, резервирование связи, используя коммуникационное промышленное оборудование. В случае выхода из строя какого-то сегмента система сохраняет работоспособность с выводом информации о неисправностях. Современные технологии ориентированы на построение систем, с одной стороны, максимально интегрированных, а с другой – максимально автономных для сохранения работоспособности при выходе из строя какой-то части системы связи или части оборудования.

Масштабы построения таких систем могут быть самые разные. Речь может идти об одном объекте, где система реализована на нескольких одинаковых приборах или на разнородном оборудовании. Или – о более сложной системе, где идёт интеграция оборудования на территориально распределённом объекте, когда глобальная система заказчика имеет несколько удалённых друг от друга объектов.

Одна из важнейших задач сведения несколько различных подсистем на какой-то один уровень – централизация информации, собираемой с приборов. Если пожарная сигнализация имеет большую ёмкость по количеству шлейфов, датчиков, и нельзя свести всё это на один прибор, то систему строят, используя несколько одинаковых приборов. И так как информационность таких систем невелика, поток событий там не должен быть большим. Ведь система должна заявлять о себе только в случае возгорания или неисправности.

Несколько слов еще об одной проблеме. Зачастую для удобства работы оператора стремятся использовать в качестве верхнего уровня компьютер. По моему мнению, в пожарных системах этого делать не нужно, потому что общение оператора с такой системой происходит достаточно редко. Зачем ставить компьютеры, которые потом покрываются толстым слоем пыли? И потом, что такое компьютер и что такое рабочее место оператора систем безопасности? Если рассматривать его как сосредоточие каких-то подсистем в самом компьютере, то получается зависимость от компьютерного «железа». И надо понимать, что обычный офисный компьютер не предназначен для работы 24 часа в сутки семь дней в неделю. Тут же начинаются проблемы с источником питания, с вентилятором и так далее. Потом свою лепту вносит операционная система, так как сейчас это довольно сложный программный комплекс, где происходит много различных конфликтов, которые инсталлятор в силу неопытности или незнания зачастую не может решить. В любом случае, компьютер во всей этой системе даже в силу своей сложности недостаточно надёжен. В некоторых системах, в каких-то решениях вполне можно обойтись аппаратным уровнем.

Применительно к техническим средствам систем безопасности проблема интеграции весьма многогранна. Зачастую она – насущная необходимость, и тогда у проектировщиков и инсталляторов есть широкий выбор способов и оборудования для решения задачи надежной защиты объекта от прогнозируемых рисков. А в иных случаях вполне достаточно решить проблему создания сети приборов на уровне тех же «сухих контактов». Всё зависит от особенностей объекта, задачи, поставленной заказчиком, и, не побоюсь этого слова, творчества инсталляторов.

Объединение приборов в одноранговую сеть