

Применение CAN-шины

в современных системах безопасности

По принципу действия сети управления бывают распределенными или централизованными. В централизованных сетях реализован принцип ведущий/ведомый (master/slave) за счет постоянного присутствия в системе центрального контроллера, ряда интеллектуальных датчиков и ряда исполнительных устройств, как с интеллектом, так и без.

Для обеспечения связи приборов в централизованной системе (например, по интерфейсу RS-485) необходимо наличие мастер-устройства, т.е. устройства, управляющего сетью (пульта управления или компьютера), постоянно опрашивающего все сетевые устройства и переадресовывающего сообщения. В мастер-устройстве сосредоточен весь интеллект построенной сети, а следовательно, лежит вся ответственность за нормальную работу всех приборов системы, так как только внутри него принимается решение о включении (выключении) тех или иных исполнительных устройств. В случае выхода из строя (отказ пульта управления, зависание компьютера, обрыв линии и т.п.) мастер-устройства нормальное функционирование сети становится невозможным, что является серьезной проблемой для обеспечения должного уровня безопасности на современном уровне.

В 80-х годах фирмой Robert Bosch был разработан **протокол CAN (Controller Area Network)** как решение для распределенных систем, работающих в режиме реального времени, с целью его применения в автомобильной промышленности. Протокол связи полностью определен Robert Bosch GmbH в спецификации требований CAN 2.0B от 1991 года. CAN-интерфейс регламентирован международными стандартами ISO 11898 для высокоскоростных и ISO 11519-1 для низкоскоростных приложений.

Оригинальная спецификация CAN (Версии 1.0, 1.2 и 2.0A) определяет длину идентификатора 11 бит (2048 возможных вариантов). Затем технические требования были изменены, чтобы уйти от указанного ограничения, и в версии CAN 2.0B длина идентификатора может быть 11 или 29 бит (536 миллионов вариантов). Версия CAN 2.0B, во многих документах может называться расширенной версией CAN.

Сети CAN являются классическим примером распределенной на битовом уровне событийной сети.

По сравнению с другими технологиями, повышенная надежность CAN обусловлена линейностью структуры шины и равноправностью ее узлов - мультимастерностью (Multi Master Bus). CAN-сеть имеет асинхронную последовательную структуру, при использовании которой обмен информацией между приборами осуществляется не централизованно (как например в RS-485), а непосредственно между приборами, т.е. применение головного мастер-устройства не является обязательным условием функционирования системы, созданной на базе CAN-шины. Переданные в сеть сообщения и управляющие команды инициируются в зависимости от тактики работы системы и событий, происходящих на защищаемом объекте и в самой системе.

Основные положения стандарта CAN:

- в качестве среды передачи данных в CAN используется дифференциальная линия связи — витая пара (иногда оптоволоконная пара, радиоканал), сигналы по которой передаются в дифференциальном режиме, линии шины называются CANH и CANL и могут быть подключены непосредственно к устройствам, не существует никакого дополнительного

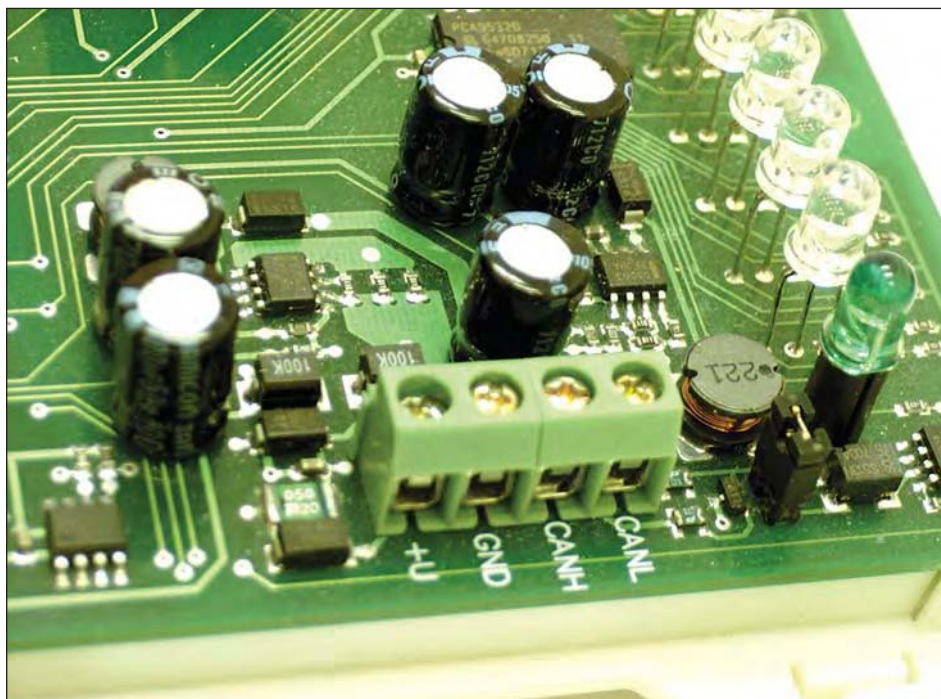


Рис. 1 Плата, поддерживающая CAN

стандарта на среду передачи данных;

- для контроля доступа к среде передачи используется метод недеструктивного арбитража;
- данные передаются короткими (максимальная длина поля данных — 8 байт) пакетами, которые защищены контрольной суммой;
- в CAN отсутствует явная адресация сообщений. Вместо этого каждый пакет снабжен полем арбитража (идентификатор + RTR-бит), которое задает приоритет сообщения в сети;
- CAN имеет исчерпывающую схему контроля ошибок, которая гарантирует повторную передачу пакета, в случае возникновения ошибок передачи/приема сообщения;
- в CAN существует способ автоматического устранения узла, являющегося источником ошибочных пакетов в сети.

Идеальным решением для любого приложения, где микроконтроллеры обмениваются сообщениями друг с другом и с удаленными периферийными устройствами является CAN. Высочайшая помехоустойчивость сетей CAN достигается благодаря подавлению синфазных помех дифференциальным приемопередатчиком, работе встроенных механизмов обнаружения ошибок, повтору ошибочных сообщений, отключению неисправных узлов от обмена по шине и устойчивости к электромагнитным помехам. Экранирование шины значительно снизит воздействие внешнего электромагнитного поля, что особенно важно для высокоскоростных режимов работы.

Гибкость построенных на базе CAN-шины систем достигается за счет простого подключения к шине и отключения от шины узлов, причем общее число узлов не лимитировано протоколом нижнего уровня. Адресная информация содержится в сообщении и совмещена с его приоритетом, по которому осуществляется арбитраж.

Система, созданная на базе приборов, поддерживающих CAN-интерфейс, является одноранговой сетью, а это означает, что любой узел CAN сети может получить независимый доступ к шине, любое сообщение может быть послано одному или нескольким узлам. Узлы могут работать в режимах «слушаю всех» (одновременно считывать сообщения) и «один говорит – остальные слушают», когда одновременно передавать данные может только один контроллер. В CAN протоколе при передаче данных приемные узлы не адресуются, а указывается идентификатор передатчика. С

помощью идентификатора указывается содержание сообщения (например, температура, задымленность и т.п.). В результате узел принимает и обрабатывает только те сообщения, которые предназначены именно для него. Идентификатор дополнительно указывает приоритет сообщения. Меньшее бинарное значение идентификатора означает более высокий приоритет сообщения.

Двоичная информация кодируется NRZ кодом: низкий уровень – 'DOMINANT', высокий уровень – 'RECESSIVE'. Для гарантированной синхронизации данных всеми узлами шины используется наполняющий бит. При последовательной передаче пяти бит одинаковой полярности, передатчик вставляет один дополнительный бит противоположной полярности перед передачей остальных битов. Приемник также проверяет полярность и удаляет дополнительные биты.

При коллективном доступе к шине используется недеструктивный арбитраж с опросом состояния шины. Перед началом передачи данных узел проверяет отсутствие активности на шине. В начале передачи сообщения узел становится управляющим шиной, все остальные узлы переходят в режим приема.

Каждый узел выдает подтверждение приема, проверяет идентификатор сообщения, обрабатывает или удаляет принятые данные. Если два или более узлов начинают передачу данных одновременно, то поразрядный арбитраж позволяет избежать конфликта на шине. Каждый узел выдает на шину свой идентификатор (старший бит формируется первым) и контролирует ее состояние. Если узел посылает 'RECESSIVE' бит и читает 'DOMINANT', значит, арбитраж потерян и узел переключается в режим приема. Это происходит тогда, когда идентификатор конкурирующего узла имеет меньшее бинарное значение. Таким образом, узел с высоким приоритетом выигрывает арбитраж, без необходимости повторять сообщение. Все остальные узлы будут пытаться передать сообщение после освобождения шины. Данный механизм не позволяет передавать одновременно сообщения с одинаковым идентификатором, поскольку ошибки могут возникнуть позже.

С 1 мая 2009 года вступает в силу Федеральный закон «Технический регламент о требованиях пожарной безопасности» №123-ФЗ. В п.5 статьи 83 сказано «Автоматические установки пожарной сигнализации должны

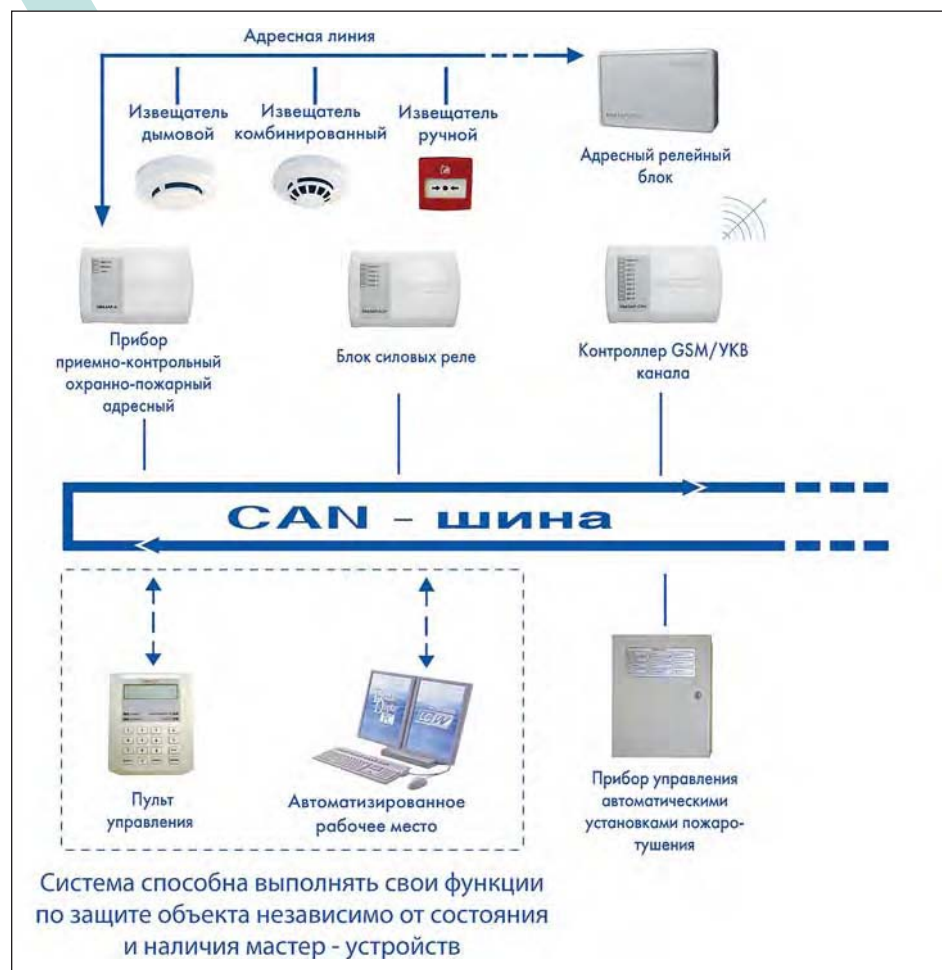


Рис. 2 Система безопасности, построенная на базе CAN-шины

обеспечивать информирование дежурного персонала об обнаружении неисправности линий связи и технических средств оповещения людей о пожаре и управления эвакуацией людей, управления системами противопожарной защиты, приборами управления установками пожаротушения". Механизм тактовых импульсов "on bus" позволяет обеспечить расширенные возможности самодиагностики состояния блоков системы безопасности, основанной на CAN, и позволяет таким системам в полной мере соответствовать букве закона.

Таким образом, использование CAN-интерфейса в системах безопасности позволяет:

- снизить нагрузку на сеть, т.к. все сообщения, передаваемые в системе событийны и принимаются сразу всеми устройствами системы;
- обеспечить высокую скорость реакции системы;
- определять коммуникационные проблемы и отказ устройств системы, используя режим подтверждения сообщений и режим самодиагностики, основанный на механизме тактовых импульсов "on bus";
- сохранить работоспособность си-

стемы при разрыве линии связи;

- подключать и отключать устройства без перенастройки других узлов системы;

- повысить надежность системы из-за возможности упрощения архитектуры сети и уменьшения числа системобразующих компонентов;

- повысить живучесть системы безопасности за счет надежного взаимодействия приборов системы, независимо от состояния и наличия мастер-устройств, и возможности построения линии связи кольцевой, радиальной и смешанной архитектуры без применения каких-либо дополнительных блоков;

- добиться уменьшения стоимости систем защиты объектов в результате применения упрощенной структуры, функционирующей без постоянного присутствия пульта управления в своем составе.

Гибкость распределенных сетей на основе CAN-шины позволяет реализовать технологию модульного построения методом проектной компоновки систем. При данном подходе возможно оптимизировать соотношение стоимость/эффективность защиты за счет:

- гибкого и экономически выгодно-

го обеспечения защиты объектов с учетом их специфики и масштабности;

- возможности легкого наращивания эксплуатируемой системы с минимальными затратами на ее модернизацию.

Системы, построенные на базе CAN-шины, могут оптимальным образом управлять большим множеством объектов, расположенных на распределенной территории. За почти 20-летнюю историю активного и успешного применения, благодаря высокой скорости передачи данных, повышенной надежности, гибкости и способности самодиагностики, CAN-шина нашла широчайшее применение как в сферах автомобильного, железнодорожного, морского и авиационного транспорта, так и в промышленной автоматике и прогрессивных системах безопасности.

А.А. Бельков, В.В. Теплов,
специальное конструкторское
бюро "Тензор"