

№1 (113), 2013 г.

Информационно-технический
журнал

Учредитель — ООО «КОМПЭЛ»

Издается с 2005 г.

Свидетельство о регистрации:
ПИ № ФС77-43993**Редактор:**Геннадий Каневский
vesti@compel.ru**Выпускающий редактор:**

Снежана Холодова

Редакционная коллегия:Андрей Агеноров
Евгений Звонарев
Сергей Кривандин
Александр Маргелов
Николай Паничкин
Борис Рудяк**Дизайн, графика, верстка:**Елена Георгадзе
Екатерина Беляева
Евгений Торочков**Распространение:**

Снежана Холодова

Электронная подписка:www.compeljournal.ru**Отпечатано:**«Гран При»
г. Рыбинск

Тираж — 1500 экз.

© «Новости электроники»

Подписано в печать:

7 февраля 2013 г.

СОДЕРЖАНИЕ

■ БЕСПРОВОДНЫЕ ТЕХНОЛОГИИ

- Невидимые сети: применение компонентов беспроводной технологии в системах охраны
Андрей Никитин 4
- Для мобильных стражей: беспроводной стандарт Bluetooth Low Energy в системах безопасности (BlueGiga)
Александр Калачев 10

■ АНАЛОГОВЫЕ МИКРОСХЕМЫ

- Для замены «таблеток»: системы РЧ-идентификации на базе компонентов RFID компании Maxim Integrated
Андрей Никитин 19
- Для RFID с интеллектуальной регистрацией: память с двойным интерфейсом от STM
Александр Калачев 23
- Передача данных без проблем: модемы и приемопередатчики от ON Semiconductor
Андрей Самоделов 30

■ МИКРОКОНТРОЛЛЕРЫ

- Защита особо важных данных при помощи аппаратной реализации механизмов AES (Maxim Integrated)
Свати Джоши 37

■ ДАТЧИКИ

- «Мы с КМОП на границе»: датчики изображения ON Semiconductor и их применение в системах безопасности
Гузелия Сафиуллина, Михаил Селезнев 39

В БЛИЖАЙШЕМ НОМЕРЕ:**ПРОДУКЦИЯ STM ДЛЯ УПРАВЛЕНИЯ ЭЛЕКТРОПИТАНИЕМ**

- Интегральные DC/DC-преобразователи
- ИС для зарядных устройств
- Программа eDesign Suite

Если вы хотите предложить интересную тему для статьи в следующий номер журнала – пишите на адрес vesti@compel.ru с пометкой «Тема в номер» или в рубрику «Я – автор» раздела «Разработчикам» сайта www.compel.ru.

ОТ РЕДАКТОРА



Уважаемые читатели!

Рад всем прошлогодним подписчикам и поздравляю новых!

Вот и прошла череда новогодних праздников, да и предсказанный конец света пролетел как-то незаметно. Наши граждане пришли в себя, оглянулись и обнаружили вокруг все те же квартиры, загородные дома, особняки, офисы, производственные помещения и прочее движимое и недвижимое имущество. И, увы — все тех же злоумышленников, от которых все это надо охранять. Невзирая ни на какие кризисы, политические и экономические. Вот почему (я, как всегда — о своем, о близком) рост рынка **систем безопасности** и, соответственно, рынка электронных компонентов для них остается стабильным все последние годы.

По данным **Информационно-аналитического Центра Современной Электроники** на конец 2011 года (более свежие данные собираются и анализируются в настоящий момент), рынок компонентов для производства систем безопасности занимает в России четвертое место (201 млн. долларов) после ВПК, промышленной электроники и систем связи, опережая такие сферы, как автоэлектроника, потребительская и медицинская электроника. Разрыв с системами связи

(205 млн.) совсем незначителен. При этом, поскольку российские преступники весьма хитроумны, а правоохранительные органы (которые тоже — не промах) своими заказами и финансированием стимулируют разработчиков, эта сфера — одна из немногих, изделия которой успешно экспортируются. И хотя наиболее массовой продукцией здесь все еще остаются старые добрые датчики пожарной сигнализации, технический прогресс не стоит на месте. Основная его примета — активное внедрение в системы безопасности беспроводных технологий. То есть символом электроники для систем безопасности теперь служит не мощная видеокамера, соединенная проводами с центральным пультом, а незаметный глазу датчик с крохотной антенной.

Именно по этой причине беспроводные компоненты занимают центральное место в нашем первом номере за 2013 год, посвященном, как легко понять из всего вышесказанного, компонентам для систем безопасности. Однако интересное в номере не ограничено беспроводной тематикой. Я бы, например, обратил внимание потенциальных разработчиков отечественных систем биометрической идентификации на материал о **КМОП-датчиках изображения** компании **ON Semiconductor** и возможности

их применения в системах безопасности.

И, если уж на то пошло, нельзя не упомянуть, что согласно маркетинговому исследованию уже упомянутого Центра Современной Электроники, компания **КОМПЭЛ** является крупнейшим в России поставщиком компонентов для производства систем безопасности. В компании работают несколько инженеров с опытом разработок именно в этой области, есть и отдельная группа продаж, «заточенная» на разработчиков и производителей таких систем. Такие компании из линейки поставок **КОМПЭЛ**, как **Texas Instruments**, **STMicroelectronics**, **Maxim Integrated**, **ON Semiconductor**, **BlueGiga**, **Digi**, **Sierra Wireless** имеют целые линейки готовых решений для разработки систем безопасности.

Как всегда, ждем ваших вопросов и обращений по материалам номера.

С уважением,
Геннадий Каневский

КОМПОНЕНТЫ ДЛЯ СИСТЕМ БЕЗОПАСНОСТИ, ПОСТАВЛЯЕМЫЕ КОМПАНИЕЙ КОМПЭЛ

Микроконтроллеры с функциями шифрования/безопасности

- Texas Instruments: DaVinci, MSP430FR59xx, Stellaris LM4F; Hercules TMS570, RM4x, TMS470M; Concerto F28M35x, F28M36x
- STMicro: STM32F2, STM32F4
- Maxim: MAX32590

Защищенные интерфейсы

- Texas Instruments
- Maxim
- STMicro
- ON Semi

Источники бесперебойного/автономного питания

- Mean Well: ADD-55, ADD-155, PSC, на DIN-рейку – DR-UPS40
- Chinfa: на DIN-рейку – DRAN/A

Контроллеры заряда батарей

- Maxim
- STMicro: STBC08, STC4054, L6924D, L6924U, STBC2, STw4102, STC3105
- ON Semi: NCP1652AG
- Chinfa: на DIN-рейку – DRU30

Датчики

- Maxim: Оптические датчики освещения/приближения, ИК-датчики MAX44000, MAX44005, MAX44008, MAX44009
- ON Semi: датчики освещенности/температуры/прикосновения

ПЗС/КМОП-матрицы/датчики

- ON Semi: VITA1300/2000/5000/25K, LUPA-300/1300-2/3000/4000, STAR250/1000, HAS-2, IBIS4-6600, MANO-9600

Модули беспроводной передачи/приема данных (GSM, ГЛОНАСС/GPS, ZigBee, Bluetooth)

- Sierra Wireless
- Digi
- Trimble
- Геостар
- Навиа
- STMicro
- BlueGiga
- Texas Instruments: CC11xx, CC24xx, CC25xx, CC2538, CC2560, CC3000

Компоненты для RFID

(специализированные контроллеры, память с беспроводным интерфейсом)

- Maxim: NFC/RFID решения: MAX66040, MAX66140; i-Button с и/ф 1-Wire
- STMicro: EEPROM M24LR, трансивер CR95HF
- ON Semi: RFID-решения NCP1080, NCP1081, ADM1032ARMZ

Аналоговые фронтэнды для газоанализаторов

- Texas Instruments: LMP9100xx



Андрей Никитин (г. Минск)

НЕВИДИМЫЕ СЕТИ: ПРИМЕНЕНИЕ КОМПОНЕНТОВ БЕСПРОВОДНОЙ ТЕХНОЛОГИИ В СИСТЕМАХ ОХРАНЫ



Охранные системы являются одной из основных областей применения беспроводных решений. Для этих приложений компания КОМПЭЛ предоставляет компоненты трех направлений беспроводных технологий: сотовая связь GSM, глобальные спутниковые системы навигации, радиосвязь технологии ZigBee. Главные бренды — Sierra Wireless, Геостар, Навиа, Trimble Navigation и Digi.

В настоящее время в охранных системах различного назначения находят применение практически весь спектр современных технологий беспроводной передачи данных. По функциональному назначению беспроводные технологии можно разделить на две группы: средства глобальных спутниковых систем навигации и средства беспроводной связи. Первая группа включает технические средства пользовательского сегмента спутниковой навигации американской системы **NavStar GPS**, отечественной системы **ГЛОНАСС**, а также совмещенные двухсистемные приемники **GPS/ ГЛОНАСС**. Ко второй группе относятся следующие технологии:

- Цифровая мобильная сотовая связь GSM, включая ряд дополнительных сервисов (GPRS, SMS, MMS и другие), а также технология широкополосной цифровой сотовой связи 3G.

- Радиосвязь в безлицензионных диапазонах (433, 868, 2400 МГц), включая технологию ZigBee и спецификации ISM-диапазона.

- Технология беспроводной связи Bluetooth различных спецификаций.

Выбор той или иной технологии беспроводной связи и, соответственно, комплекта технических средств определяется спецификой конкретного приложения. В таблице 1 приведены некоторые технические возможности

различных технологий беспроводной связи.

Применение GSM-технологий в охранных системах

Лавинообразное распространение сотовой связи, произошедшее в течение последних 10-15 лет, не могло не оказать влияние на тенденции развития систем безопасности. Широкое применение встраиваемых GSM-модулей в охранных системах обусловлено следующими факторами:

- Передача «тревожных» сообщений, в принципе, не ограничивается расстоянием: важно, чтобы охраняемая система и получатель сообщения находились в зоне действия сети. Если учесть, что международный роуминг в настоящее время перестал быть экзотикой, то получатель может находиться в любой обитаемой точке планеты. В то же время любые технологии радиосвязи имеют конечный радиус действия.

- Промежуток времени между отправкой сообщения и его приемом, как правило, не превышает минуты, что вполне приемлемо для большинства охранных систем.

- Сотовая связь не бесплатна, но вполне доступна по стоимости для любых приложений.

- Стоимость встраиваемых GSM-модулей невелика даже для малобюджетных проектов.

- Помимо голосовой связи и отправки SMS-сообщений, возможны и другие форматы передачи данных (GPRS, EDGE, HSPA и другие). Развитие технологий широкополосной цифровой сотовой связи 3G позволяет существенно повысить скорость передачи данных и, соответственно, увеличить объем передаваемой информации, что, в свою очередь, расширяет возможные области применения технологий сотовой связи.

- Технология программирования GSM-модемов не требует особых интеллектуальных усилий: механизм использования AT-команд достаточно прост. Конкретный набор и синтаксис команд для определенного типа модема может быть оригинальным, но общие принципы применения AT-команд сохраняются для любой модели.

- GSM-технология является весьма экономичной с точки зрения мощности, потребляемой модемом в дежурном режиме.

Рассмотрим наиболее популярные применения GSM-технологий в охранных системах:

- Онлайн мониторинг транспортных средств с использованием технологий спутниковой навигации GPS/ ГЛОНАСС.

- Охранные и противопожарные системы зданий, складов, территорий и других охраняемых помещений. Сюда же можно отнести охранные системы дач, гаражей и другой недвижимости. Принцип действия систем автономной сигнализации — срабатывание «тревожного» датчика вызывает отсылку SMS-сообщения. В качестве такого датчика могут использоваться датчики присутствия, PIR-датчики движения, концевые датчики открытия окон и дверей, датчики дыма, температуры и др.

Таблица 1. Сравнительные характеристики различных технологий беспроводной связи

Диапазон, МГц	Выходная мощность, мВт	Расстояние, км	Скорость в радиоканале, кбит/сек	Реальная скорость передачи данных, кбит/сек
433/868	10...25	до 5	до 1000	до 500
ZigBee 2400	1...100	до 2	250	до 40
Bluetooth	2,5...50	до 1	3 000	до 460 (SPP)
GSM/GPRS/EDGE	1000...2000	до ~30 от БС	до 384	9,6...200
3G	250	до ~8 от БС	до 42 000	тысячи

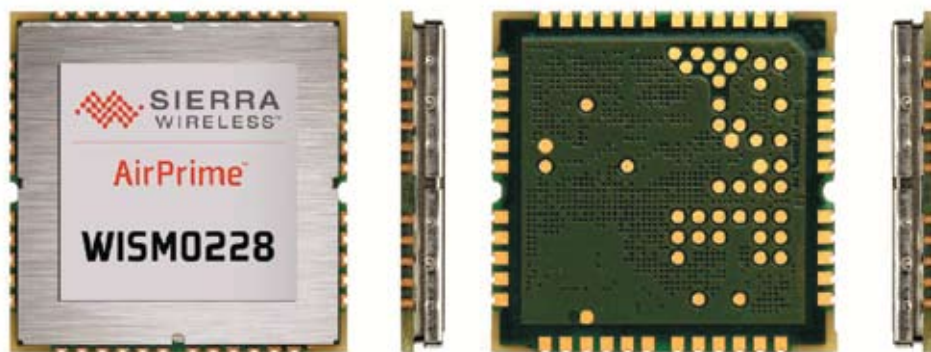


Рис. 1. Конструктивное исполнение модулей WISMO218 и WISMO228

- Системы управления и контроля доступа. Например, если общеобразовательная школа оборудована системой контроля доступа, то, как опция, может обеспечиваться отправка SMS-сообщений на указанный номер при появлении ребенка в школе и уходе из нее. Кроме того, в системах контроля доступа распределенных территорий отправка SMS-сообщений на центральный пункт охраны может применяться при попытках доступа на неохранные территории и помещения.

- Системы оповещения и дозвола при тревогах и чрезвычайных ситуациях, компоненты связи систем типа «Умный Дом», системы сбора данных (например, АСКУЭ), системы телеметрии различного назначения и многое другое.

Необходимо отметить, что применение GSM-технологий ограничено, главным образом, пассивными охраняемыми системами. То есть, системами, задачей которых является привлечение внимания охранных служб или собственника к факту возникновения нештатной ситуации на охраняемом объекте или оповещение его о выполнении некоего прогнозируемого события (например, прохождения автотранспортом оговоренной контрольной точки). В активных охранных системах GSM-технологии могут использоваться лишь в качестве второстепенной, дополнительной опции.

Продукция Sierra Wireless в области GSM-технологий для встраиваемых систем

Линейка GSM-модемов, предлагаемых компанией КОМПЭЛ, представлена канадской компанией **Sierra Wireless**. После объединения с извест-

ной французской компанией **Wavecom** Sierra Wireless стала крупнейшим мировым производителем в области GSM-модулей для встраиваемых систем, существенно опережая компании **Cinterion**, **Telit Communication** и другие.

В продукции Sierra Wireless направление GSM-модулей для встраиваемых систем представлено семейством **AirPrime**, которое, в свою очередь, включает несколько серий GSM-модулей второго, третьего и четвертого поколений (2G, 3G и 4G) различного назначения и конструктивного исполнения. Модули серий **Q24** и **Q26**, модемы **Fastrack** и **Integra** в свое время получили заслуженное уважение у разработчиков охранных систем. Эти изделия продолжают применяться и в настоящее время, но сегодня наибольший интерес вызывают новые изделия из серии **WS**, а именно — миниатюрные, удобные в интеграции 2G-модули **WS6318**, **WISMO218** и **WISMO228**.

Модули **WISMO218** и **WISMO228**, представленные на рисунке 1, выполнены в SMD-корпусе типа LCC размера 25x25 мм с краевыми контактами, то есть пригодны не только для автоматической пайки на плату, но допускают также и ручную пайку. Модуль **WISMO218** является двухдиапазонным, предназначенным для использования в мобильных сетях Европы, Азии, Африки и Австралии (то есть 900/1800 МГц). Модуль **WISMO228** с функциональной точки зрения является аналогом **WISMO218**, но является четырехдиапазонным, то есть, помимо диапазонов 900/1800 МГц, поддерживает также пару 850/1900 МГц и может быть использован, кроме того, для работы с сетями мобильных операторов Америки. Учитывая тот факт, что цены модулей **WISMO218** и **WISMO228** одинаковы, а **WISMO228** закрывает все функциональные возможности **WISMO218**, в дальнейшем будем упоминать только модуль **WISMO228**. С точки зрения архитектуры модули имеют полноценную реализацию TCP/IP-стека, поддерживают обмен по последовательному интерфейсу UART, имеют 11 линий ввода-вывода

общего назначения, часы реального времени, сигнал готовности модуля, выход для светодиодной индикации, выход ШИМ (генератор звукового сигнала вызова) и интерфейс SIM-карты. Аудиосистема модуля включает один аналоговый вход с микрофона и один аналоговый выход на динамик, поддерживает функции эхо- и шумоподавления, звуковой кодек поддерживает спецификации HR, FR, EFR и AMR. Управление модулем осуществляется посредством AT-команд.

Модуль **WS6318**, представленный на рисунке 2, на данный момент является самым миниатюрным 2G-модулем из представленных на рынке. Он выполнен в SMD-корпусе размером 15x17,8 мм и, таким образом, занимает на плате всего 267 мм², что по сравнению с модулями **WISMO228** обеспечивает экономию площади более, чем на 55%. Отметим, что модуль реализован в корпусе типа LCA, то есть, в отличие от **WISMO**, допускается только автоматическая пайка на плату. Модуль **WS6318** является двухдиапазонным, то есть не предназначенным для работы в мобильных сетях Америки (в отличие от **WISMO228**). Функционально **WS6318** обеспечивает те же возможности, что и модуль **WISMO228**, но аудиосистема **WS6318** имеет дополнительные функции. Добавлены второй аналоговый выход на динамик и цифровой аудиointерфейс PCM. Реализована функция декодирования DTMF-сигнала (двухтональный многочастотный аналоговый сигнал, используемый для набора телефонного номера). Помимо стека TCP/IP реализован протокол передачи файлов FTP. Управление осуществляется через AT-команды, большая часть которых (но не все) совпадает с набором команд модулей **WISMO228**. Отличительной особенностью конструктивного исполнения является уникальная технология покрытия модуля, которая делает его более устойчивым к воздействию агрессивных условий внешней среды. Диапазон рабочих температур -40...+85°C.

Компания-производитель обеспечивает модули семейства **WS** необходимыми средствами отладки для изучения возможностей изделий, упрощения разработки аппаратных и программных средств. Кроме того, в фирменных материалах даны необходимые рекомендации для разводки печатной платы, подключения источников питания, аудиоустройств, внешней антенны, а также — по другим тонкостям, которые могут вызвать затруднения у пользователя.

Модули **WISMO228** и **WS6318**, являясь устройствами начального уровня, обеспечивают необходимый для большинства приложений набор функциональных возможностей при невысокой стоимости, что обеспечивает привлека-



Рис. 2. Конструктивное исполнение модуля WS6318

тельность этих изделий по сравнению с аналогичными по назначению устройствами других производителей.

Более подробную информацию о продукции Sierra Wireless в области GSM-технологий можно найти в литературе [1-3].

Применение спутниковой навигации в мониторинге транспорта

Спутниковый мониторинг (или GPS-мониторинг) транспорта — система отслеживания нахождения транспортных средств, в основе которой лежит использование технологий глобальных спутниковых систем навигации (главным образом — американской системы NavStar GPS, отечественной системы ГЛОНАСС, или их совмещенного варианта). Отметим, что обеспечение безопасности транспортных средств в узком смысле, то есть защита их от угона средствами спутникового мониторинга возможна и нередко реализуется, но не является главной. В традиционном, более широком, смысле спутниковый мониторинг обеспечивает охрану интересов собственников транспортных компаний от различного рода злоупотреблений персонала. Существуют два варианта спутникового мониторинга транспорта: онлайн и оффлайн. При онлайн-мониторинге данные о местонахождении транспортного средства с определенной периодичностью отсылаются на диспетчерский пункт с помощью GSM-модема (например, в виде SMS-сообщений). В этом случае диспетчер имеет сведения о положении транспорта в реальном времени (с учетом дискретности в посылке сообщений) и, соответственно, информацию об отклонении от заданного маршрута и других нештатных ситуациях получает с минимальным опозданием. В режиме оффлайн данные в процессе маршрута записываются в накопитель данных, а по прибытии на диспетчерский пункт передаются диспетчеру для контроля. Механизм передачи данных может быть беспроводным (ZigBee, WiFi, Bluetooth и другие) или контактным (флеш-накопитель, смарт-карта), но сути дела не меняет: данные доступны для контроля после успешного возвращения домой.

Навигационный приемник (GPS-приемник), непрерывно получая сигналы с навигационных спутников, обрабатывает их и, при наличии качественных сигналов от достаточного числа спутников, получает так называемое «решение», то есть координаты приемника в системе «широта, долгота, высота от уровня моря» и время, которому соответствует решение. Как вторичные результаты могут быть рассчитаны скорость и курс движения, а также обобщенные параметры качества решения. Эта информация при контроле (онлайн или оффлайн)

позволяет однозначно зафиксировать отклонения от заданного маршрута (например, «левые» поездки), несоблюдение установленного режима движения (немотивированные остановки, систематическое превышение скорости и прочее). В большинстве случаев бортовой контроллер анализирует состояние дополнительных датчиков, фиксирующих уровень топлива в баке, нагрузку на ось транспортного средства, температуру в холодильнике, нажатие «тревожной» кнопки, другие параметры и события, которые также записываются в протокол и позволяют контролировать добросовестность водителя. На практике управляющие транспортными компаниями отмечали, что внедрение средств мониторинга сэкономило 10...30% топлива и наводило элементарный порядок в отношении дисциплины.

Первые системы спутникового мониторинга транспорта появились в странах бывшего СССР примерно в 1997 году и были ориентированы исключительно на спутники системы NavStar GPS (отечественная система ГЛОНАСС была в совершенно «разобранном» состоянии). Соответственно, в треках использовались приемники только GPS и, преимущественно, зарубежных производителей. Но в августе 2008 года было принято постановление Правительства РФ «Об оснащении транспортных, технических средств и систем аппаратурой спутниковой навигации ГЛОНАСС или ГЛОНАСС/GPS» [4], которое обязало использовать систему ГЛОНАСС в том числе:

- на морских судах и судах внутреннего речного и смешанного («река-море») плавания;
- на автомобильных и железнодорожных транспортных средствах, используемых для перевозки пассажиров, специальных и опасных грузов;
- на технических средствах, образцах вооружения, военной и специальной технике, предназначенной для Вооруженных Сил РФ (и приравненных к ним ведомств).

В тот момент времени слова «система ГЛОНАСС» уже не были пустым звуком, и добавление российской системы к американской давало существенное улучшение качества работы. Кроме того, возможность применения трекеров «только GPS» стала весьма ограниченной. Естественно, что с этого момента стал расти интерес к российским производителям совмещенных приемников ГЛОНАСС/GPS.

Модули приемников ГЛОНАСС/GPS компании «ГеоСтар навигация»

Московская компания КБ «ГеоСтар навигация» предлагает на рынок приемники ГЛОНАСС /GPS OEM-типа (то есть, предназначенные для интеграции в конечную аппаратуру пользователя).



Рис. 3. ГЛОНАСС/GPS-приемники GeoC-3 (слева) и GeoC-3M

Приемники GeoC-1 и GeoC-1M отличаются типом исполнения (поверхностный или объемный монтаж) и, соответственно, габаритами плат. Данные приемники были подробно рассмотрены ранее [5], поэтому перейдем к их дальнейшему развитию — приемникам GeoC-3 и GeoC-3M, которые появились на рынке в 2012 году.

Приемники GeoC-3 и GeoC-3M выведены на рынок в 2012 году и являются дальнейшим развитием GeoC-1x. Принципиальными изменениями является добавленная дополнительно к созвездиям ГЛОНАСС/GPS возможность работы с европейской геостационарной спутниковой навигационной системой EGNOS и американской глобальной системой распространения дифференциальных поправок WAAS. Как следствие, число каналов увеличено до 32. Это, естественно, повышает точность решения как в плане, так и по вертикали, однако на данный момент пять спутников WAAS обслуживают только большую часть территории США и Канады, а система EGNOS в настоящее время не обеспечивает покрытие территории РФ (на практике есть некоторое покрытие для самых западных областей). Иными словами, новые функциональные возможности сделаны с расчетом «на вырост». Добавлена возможность работы в дифференциальном режиме (при наличии источника дифференциальных поправок), несколько повышена точность решения (до 2,5 метров в плане и 3,5 метров по высоте). Также уменьшено время получения первого решения при «холодном» и «горячем» старте. Модификации GeoC-3 и GeoC-3M, представленные на рисунке 3, функционально идентичны и имеют только конструктивные отличия.

Компания «ГеоСтар-навигация» для поддержки разработчиков предлагает также отладочные средства и демонстрационные платы, пакеты демонстрационных программ и необходимые аксессуары (антенны, переходники и прочее) для создания пользователем законченных изделий.

Модули приемников ГЛОНАСС/GPS компании Навиа

Санкт-Петербургская компания Навиа предлагает совмещенный ГЛОНАСС/GPS 32-канальный приемник



Рис. 4. ГЛОНАСС/GPS-приемник ML8088s

ML8088s, представленный на рисунке 4. Существенные функциональные особенности данного изделия:

- В основе приемника лежит микросхема **STA8088FG** семейства **Teseo II** — новейшая разработка компании **STMicroelectronics**. В данной разработке реализованы самые современные технологии обработки сигнала спутников и получения навигационного решения: прогнозирование информации по технологии **ST-AGPS**, трехуровневая система подавления помех и ряд частных решений, обеспечивающих снижение времени получения первого решения, повышение чувствительности, снижение потребляемой мощности.

- Помимо совмещенного созвездия ГЛОНАСС/GPS, приемник (а точнее — микросхема **STA8088FG**) поддерживает созвездие спутников **GALILEO** — спутниковую навигационную систему Евросоюза. Предполагается, что система войдет в строй в 2014-2016 году и будет доступна на территории стран бывшего СССР. Сложно предсказать, как сильно улучшится при этом точность позиционирования, но в этом случае надежность непрерывного получения навигационного решения в условиях «городских джунглей» предположительно достигнет значения более 95% в любое время суток.

- Приемник поддерживает также проектируемую японскую систему навигационных поправок **QZSS**. Однако, учитывая тот факт, что покрытие системы ограничится регионом от Японии до Австралии, данная особенность для российского потребителя существенной роли не играет.

На данный момент (при работе от созвездия ГЛОНАСС/GPS) обеспечивается следующая точность определения координат: в плане — 3 метра, по высоте — 4 метра. Точность определения ско-

рости — 0,05 м/с. Каналы обмена данными: два дуплексных канала RS232 (уровни сигналов LVTTTL). Обмен данными с приемником осуществляется по протоколу компании **STMicroelectronics**, подобному NMEA 0183, бинарный протокол не применяется. Для поддержки разработчика компания-производитель предлагает также необходимые средства отладки и программное обеспечение.

Модули приемников ГЛОНАСС/GPS компании Trimble Navigation

Американская компания **Trimble** — давно и хорошо известный бренд на рынке систем спутниковой навигации. В линейке OEM-приемников компания предлагает семейство модулей **Condor** и модули **Copernicus II**. Все приемники обеспечивают примерно равные рабочие характеристики: первое решение — не более 38 секунд в «холодном» старте и 2 секунды в «горячем» старте. Точность определения координат в плане — 2 метра, по высоте — 3 метра. Приемник выдает метки времени с точностью 25 нсек. Различия между шестью типами модулей **Condor** — в конструктивном исполнении и сервисных функциях: поддержка пассивной антенны, определение факта подключения антенны, наличие порта USB, вывод управления режимом Standby. Модули **Condor** поддерживают спутниковые системы EGNOS и WAAS, а также используют технологию прогнозирования AGPS. В качестве протокола обмена данными используется стандартный вариант NMEA 0183 по каналу RS232. Модули **Copernicus II** также поддерживают EGNOS и WAAS, но не используют технологию AGPS. Кроме стандартного варианта NMEA 0183 в модулях **Copernicus II** используются также традиционные для Trimble протоколы TSIP и TAIP, популярные в первые годы освоения GPS-технологий.

К сожалению, сегодня в изделиях Trimble не обеспечивается поддержка отечественной спутниковой системы ГЛОНАСС. Однако в ближайших планах компании Trimble предполагается выпуск на рынок своего ГЛОНАСС/GPS-модуля на чипсете **STA8088FG**.

Технология ZigBee и области ее применения

ZigBee — технология построения беспроводных сетей передачи данных, объединяющих значительное количество узлов, которые обмениваются между собой небольшими объемами информации. Технология ZigBee основана на двух независимых документах:

- Стандарт IEEE 802.15.4 определяет два уровня стека. Самый нижний уровень **PHY** — физические параметры радиоканала (диапазон частот, число каналов, тип модуляции, параметры сигналов) и следующий уро-



Рис. 5. Взаимосвязь стандарта IEEE 802.15.4 и стека ZigBee

вень MAC — протокол доступа к среде (структура посылки по радиоканалу, систему адресации, механизмы проверки и подтверждения целостности данных, механизм урегулирования коллизий). Фраза «IEEE 802.15.4» не относится только к технологии ZigBee. Это физико-логическая база, на которой построена технология ZigBee, но не только она.

- Спецификация стека ZigBee определяет три следующих уровня стека: уровень канала передачи данных **DLC**, который оговаривает формирование и контроль пакетов данных, управление потоком данных; сетевой уровень **NWK** решает задачи безопасности сети, трансляции и маршрутизации сообщений, обработки сетевых процедур, поддержки различных топологий; уровень поддержки приложений **APS** отвечает за безопасность устройства, трансляцию сообщений и организацию сервисов устройств. Профили приложения частично оговорены в спецификации ZigBee, а частично оставлены на усмотрение производителя оборудования. Иными словами, спецификация ZigBee определяет совокупность правил, по которым будут взаимодействовать устройства, объединенные в сеть. ZigBee является некоторой программной надстройкой, опирающейся на стандарт IEEE 802.15.4. Взаимосвязь стандарта IEEE 802.15.4 и стека ZigBee представлена на рисунке 5.

Топология сетей ZigBee может быть самой разнообразной: «точка — точка», «звезда», «дерево», а также произвольная ячеистая топология (или топология mesh). Различные варианты топологии представлены на рисунке 6. Технология ZigBee обеспечивает возможность организации сложных децентрализованных ad-hoc (образованных случайными абонентами)-структур. В таких сетях каждый узел напрямую связан с несколькими другими узлами, эти связи могут обновляться и оптимизироваться при отключении устройств от сети или при появлении новых. При разрушении существовавшего маршрута (авария, отключение маршрутизатора от сети) автоматически формируются новые маршруты передачи данных в обход отключенного узла (если это возможно).

Спецификацией ZigBee предусмотрено три типа узлов (устройств): координатор, маршрутизатор и оконечное устройство. Координатор инициализирует сеть и управляет сетевыми узлами, а в процессе работы может быть источником, приемником и ретранслятором сообщений. Маршрутизатор отвечает за выбор пути доставки сообщения, передаваемого по сети, и, в процессе работы, также может быть источником, приемником или ретранслятором сообщений. Оконечное устройство не участвует в

управлении сетью и ретрансляции сообщений, являясь только источником или приемником сообщений.

Области применения сетей ZigBee:

- Автоматизация коммерческих зданий. Данная технология используется для сбора и обработки информации от датчиков различного назначения: температуры, влажности, освещения, вентиляции и прочее.
- Системы охранной и пожарной безопасности: сбор и обработка информации от устройств пожарной сигнализации, датчиков присутствия, движения, освещенности, концевых выключателей дверей и окон.
- Системы контроля и управления доступом (в качестве сети, объединяющей аппаратуру «точек доступа» и контрольный пульт).
- Системы контроля и мониторинга автотранспорта в автопарках: транспортный мониторинг в режиме оффлайн.
- Системы учета и логистики грузов на крупных складах и базах. В этом случае подразумевается применение технологии RFID-идентификаторов.
- Системы промышленного контроля, автоматизации и телеметрии производственных процессов.
- Домашняя автоматизация и системы «Умный дом».

Основные преимущества технологии ZigBee:

- Технология обеспечивает крайне низкое энергопотребление. Большую часть времени устройство проводит в режиме сна, включаясь лишь в моменты приема или передачи данных. Экономичность устройств ZigBee позволяет им работать автономно с питанием от батарей в течение нескольких лет.

- ZigBee сегодня — единственная высокоуровневая технология беспроводной передачи данных, которую поддерживает большое количество компаний-производителей.

- Присутствие на рынке множества независимых производителей однотипного по назначению оборудования обеспечивает разумный уровень цен на компоненты.

- Применение аппаратуры ZigBee в Российской Федерации в частотном диапазоне 2,405...2,485 ГГц не требует получения частотных разрешений и дополнительных согласований.

По технологии ZigBee существует достаточное количество литературных материалов. В качестве обзорного введения в технологию можно рекомендовать учебное пособие [6], а также многочисленные материалы на сайте компании КОМПЭЛ.

Модули ZigBee компании Digi

Американская компания Digi International производит широкий спектр устройств беспроводной связи для работы в диапазонах частот 800...2400 МГц. В этой номенклатуре можно выделить четыре основных направления:

- Радиомодули для встраивания в аппаратуру пользователя (ОЕМ-продукты).
- Законченные модемы для передачи данных по радиоканалу.
- Беспроводные датчики и преобразователи интерфейсов (адаптеры).
- Межсетевые шлюзы ZigBee — Ethernet и Bluetooth — Ethernet.

Применительно к тематике данной статьи особый интерес вызывает первое направление, в котором, в свою очередь, можно выделить следующие семейства изделий:

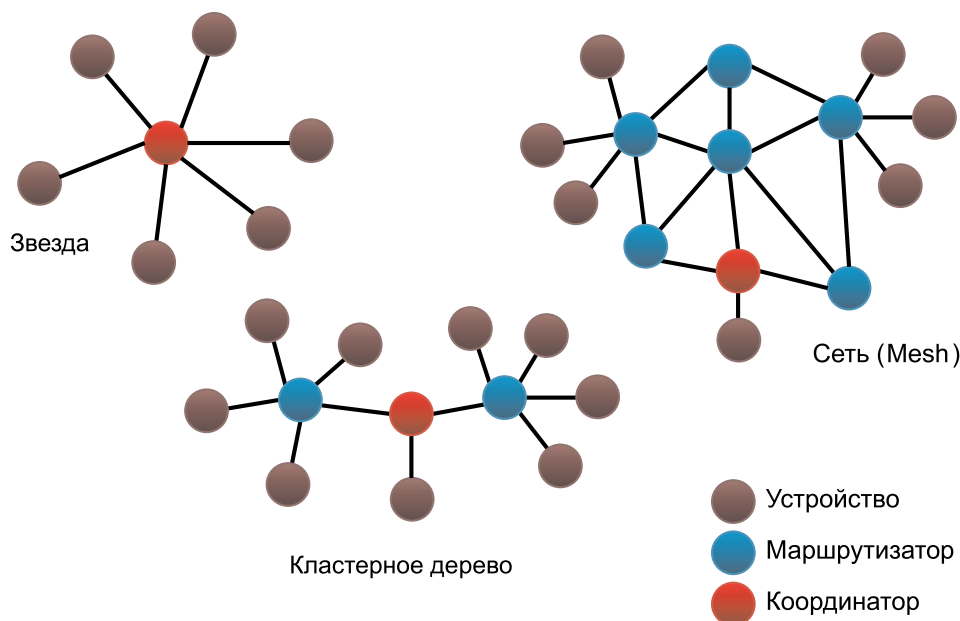


Рис. 6. Различные варианты топологии сетей ZigBee



Рис. 7. Модули XBee компании Digi

• Высокочастотные радиомодули **XBee 802.15.4** (или Series 1), поддерживающие только требования стандарта IEEE 802.15.4.

• Радиомодули **XBee ZB** и **XBee-Pro ZB** (или Series 2), которые поддерживают не только стандарт IEEE 802.15.4., но и спецификацию ZigBee.

• Радиомодули **XBee ZB SMT** и **XBee-Pro ZB SMT** (или Series S2C), поддерживающие стандарт IEEE 802.15.4. и спецификацию ZigBee, предназначенные для поверхностного монтажа на плату.

• Радиомодули **XBee 868LP**, предназначенные для работы в безлицензионном диапазоне 868 МГц, с пониженным энергопотреблением, для поверхностного монтажа на плату.

• Радиомодули **XBee Wi-Fi**, предназначенные для работы в безлицензионном диапазоне 2400 МГц по требованиям ISM (*Industrial, Scientific and Medical*). Диапазон ISM — так называемый частотный диапазон для промышленных, научных и медицинских приложений. Изделия, предназначенные для работы по требованиям спецификаций ISM, стандарту IEEE 802.15.4. не соответствуют, несмотря на использование той же частоты 2400 МГц.

Варианты конструктивного исполнения модулей различных серий представлены на рисунке 7.

Каждая из серий включает в себя различные модификации. Например, передача данных может осуществляться посредством бескорпусной чип-антенны, либо антенна может быть выпаянна в виде проводника-змейки на печатной плате, модуль может содержать разъем для подключения съемной антенны или для подключения антенного кабеля (переходника). Возможные варианты исполнения довольно разнообразны, ознакомиться с ними можно на сайте производителя. Отметим также, что для каждой серии производитель предлагает отладочный комплект (а иногда и не один) с соответствующим программным обеспечением.

Поскольку наибольший интерес представляют ZigBee-модули, рассмотрим подробнее устройства XBee ZB и XBee-Pro ZB. Модули XBee ZB обеспечивают дальность связи до 40 метров в

помещении и до 120 метров в условиях прямой видимости при мощности передатчика до 2 мВт. В качестве интерфейса управления используется последовательный канал обмена UART, кроме этого, модуль содержит 4-канальный аналого-цифровой преобразователь и 10 цифровых линий ввода-вывода общего назначения, которые предназначены для подключения аналоговых и/или дискретных датчиков. Управление осуществляется либо при помощи AT-команд (так называемый прозрачный режим), либо с использованием API-фреймов. Строго говоря, в каждый модуль при изготовлении записывается определенная прошивка *firmware*, которая определяет, во-первых, роль устройства в сети — координатор или маршрутизатор (оконечное устройство), и, во-вторых, способ управления — AT-команды или API-фреймы. Прошивка модуля может быть изменена пользователем при помощи специальной утилиты, но в любом случае в рамках одной сети должен использоваться единый метод управления. Модули могут работать в спящем режиме, в этом случае оконечное устройство будет находиться в режиме низкого энергопотребления и выйдет из него при получении посылки или при возникновении необходимости передать свои данные. Модули XBee-Pro ZB (Series 2) являются дальнейшим развитием XBee ZB. Они обеспечивают дальность связи в помещении до 90 метров, а в условиях прямой видимости — до 3200 метров при мощности передатчика до 63 мВт. Кроме того, введены дополнительные блоки встроенной памяти 32 кбайта EEPROM и 2 кбайта ОЗУ.

ZigBee-модули компании Digi являются законченным решением («кирпичиком») для построения сети ZigBee. Применение модулей не предполагает детального изучения пользователем спецификации ZigBee и программирования модуля, благодаря этому создание работающей сети возможно при минимальных затратах времени.

Заключение

За последние пять лет каждое из трех рассмотренных направлений беспроводных технологий сделало существенный шаг вперед, что не могло не сказаться на

возможностях их применения в охран-ных системах. Модули GSM-связи даже второго поколения были значительно миниатюризированы и в настоящее время конструктивно оформлены не в виде отдельных плат или небольших устройств, а в виде микросборок площадью в несколько квадратных сантиметров, что, в свою очередь, минимизирует габариты конечных устройств (а, следовательно, повышает их скрытность). Модули третьего и четвертого поколений позволили значительно повысить объем передаваемой информации. Помимо привычных SMS-сообщений, появляется возможность передавать абоненту по сотовой связи изображения или короткие видеоролики с систем видеонаблюдения. Успешное развитие российской навигационной системы ГЛОНАСС инициировало интерес к разработке совмещенных навигационных приемников и, как следствие, повысило надежность работы средств мониторинга транспортных средств в условиях сложной местности. Технология беспроводной связи ZigBee из просто перспективного направления выросла в целый ряд проектов беспроводных сетей с динамической конфигурацией. Номенклатура беспроводных компонентов, предлагаемых компанией КОМПЭЛ, непрерывно отслеживает последние изменения у производителей, что дает возможность пользователю выбрать решение, оптимальное как по функциональным, так и по ценовым критериям.

Литература

1. Пушкарев О. Обзор продукции Sierra Wireless для беспроводной передачи данных // *Новости электроники*, №10, 2009.
2. Пушкарев О. Миниатюрный GSM-модуль WS6318 // *Электронные компоненты*, №2, 2012.
3. Встраиваемые беспроводные модули Sierra Wireless AirPrime™ серии WS Series // *Материал компании Sierra Wireless*.
4. Постановление Правительства Российской Федерации от 25 августа 2008 г. «Об оснащении транспортных, технических средств и систем аппаратурой спутниковой навигации ГЛОНАСС или ГЛОНАСС/GPS» // *страница в Интернете* <http://www.aggf.ru/proekt/zakon/doc.php?zakID=6>.
5. Никитин А. Совмещенные приемные модули систем ГЛОНАСС/GPS производства КБ «Геостар Навигация» // *Новости электроники*, №4, 2010.
6. Балонин Н.А., Сергеев М.Б. Беспроводные персональные сети на основе ZigBee / учебное пособие. — СПб: ГУАП, 2012. — 58 с. 

Получение технической информации,
заказ образцов, поставка —
e-mail: wireless.vesti@compel.ru

Александр Калачев (г. Барнаул)

ДЛЯ МОБИЛЬНЫХ СТРАЖЕЙ: БЕСПРОВОДНОЙ СТАНДАРТ BLUETOOTH LOW ENERGY В СИСТЕМАХ БЕЗОПАСНОСТИ



Учет прихода работников и проверка прав доступа. Автоматическая блокировка оборудования или предупреждение об опасности на промышленном объекте. Слежение за маленьким ребенком в местах скопления людей. Установление местонахождения владельца багажа. Все эти задачи решают мобильные системы охраны, контроля и безопасности на базе беспроводных модулей BlueGiga стандарта Bluetooth Low Energy (BLE).



Пожалуй, одной из наиболее часто встречающихся в повседневной жизни беспроводных сетевых технологий (после сотовой связи) является Bluetooth. Благодаря относительно высоким скоростям передачи данных и неплохим энергетическим показателям технология Bluetooth получила широкое распространение в мобильных электронных устройствах, персональных компьютерах, ноутбуках, беспроводных наушниках, гарнитурах, мультимедийных центрах. Стандарт позволяет поддерживать достаточно разветвленную и сложную сеть устройств. Однако, для применения в сенсорных сетях классический Bluetooth подходит мало из-за значительного для автономных источников питания энергопотребления вследствие особенностей работы стека протоколов.

Технология Bluetooth Low Energy (BLE) [1-3] — Bluetooth 4.0 является технологией беспроводной связи для ближних коммуникаций, разработанной группой Bluetooth Special Interest Group (SIG). В отличие от предыдущих стандартов — Bluetooth 2.0, Bluetooth 2.1 + EDR, Bluetooth 3.0, стандарт BLE изначально ориентирован на применение в системах сбора данных, мониторинга с автономным питанием. В отличие от технологий сенсорных сетей, таких как, ZigBee, 6LoWPAN или Z-Wave, ориентированных на разветвленные распределенные сети с многочисленными передачами данных между узлами сети, Bluetooth Low Energy рассчитан на топологии типа «точка-точка» и «звезда». Основными областями применения BLE являются устройства обеспечения безопасности, управления электроприборами и отображения показаний, датчики с батарейным питанием, домашние медицинские приборы, спортивные тренажеры.

Успех предыдущих версий Bluetooth, подтвержденный массовым применением беспроводных интерфейсов данных стандартов в большом количестве устройств, в том числе — рассчитанных на обычного потребителя, позволяет ожидать аналогичной ситуации и с устройствами, поддерживающими стандарт BLE. В частности IETF 6LoWPAN Working Group рассматривает BLE как одну из значительных составляющих т.н. «Интернета вещей» (Internet of Things) и разрабатывает спецификацию, позволяющую транслировать пакеты IPv6 посредством BLE [2, 3].

Компания BlueGiga является одной из первых компаний, которая начала внедрять технологию Bluetooth Low Energy в своих устройствах. Однорежимные устройства (single-mode) выпускаются с 2010 года, а с 2011 года — и двухрежимные (dual-mode). Аккорпмент устройств с технологией Bluetooth Low Energy от BlueGiga позволяет строить на их основе решения для самых различных секторов рынка встраиваемых беспроводных устройств:

- спортивное оборудование и аксессуары — измерители пульса, шагомеры, регистраторы ритма — выполненные в виде наручных часов, браслетов;
- датчики — температуры, влажности, присутствия;
- системы сбора и отображения данных;
- бытовые медицинские устройства — весы, тонометры, глюкометры, датчики температуры, дистанционные устройства вызова (в частности, т.н. «радионяни»);
- устройства бытовой электроники — пульты и консоли управления, беспроводные устройства ввода (мышь, клавиатуры, графические планшеты);
- средства автоматизации — части систем домашней автоматизации, в част-

ности, шлюзы между домашней сенсорной сетью и мобильными телефонами с Bluetooth;

• информационные устройства — распространение информации о помещениях, объектах, отделах посредством широкоэмиттерных сообщений.

Отдельно можно выделить возможность применения BLE-модулей BlueGiga в устройствах обеспечения безопасности. Это могут быть тревожные кнопки, бесконтактные ключи, выполненные в виде отдельных брелоков или функционирующие на базе мобильных телефонов.

Ряд задач может быть решен на основе обнаружения присутствия других BLE-устройств в радиусе действия сигнала центрального узла. К таким решениям относятся устройства-сигнализаторы, позволяющие обнаруживать удаление владельца от сумочек, багажа, кошельков, портмоне со встроенным BLE-модулем и сигнализирующее ему и окружающим (при необходимости) о потере владельца. Модули серий **BLE111**, **BLE112** благодаря своим компактным размерам, низкому профилю и малому потреблению позволяют встраивать сигнализирующие устройства непосредственно в предметы (карманы сумочек, корочки кошельков и записных книжек, стенки портфелей). Будучи встроенными в браслеты или брелоки, подобные устройства помогут, к примеру, не потерять ребенка в местах с большим скоплением людей (рынки, вокзалы, супермаркеты, аэропорты). Как бы это ни казалось странным, но такая проблема существует.

Аналогичным образом BLE-устройства могут служить для учета времени прихода/ухода работников: они устанавливаются на входе или выдаются по приходу на работу. Возможна также реализация систем мониторинга присутствия:

- в случае офисного применения — проверка прав доступа работника к дан-

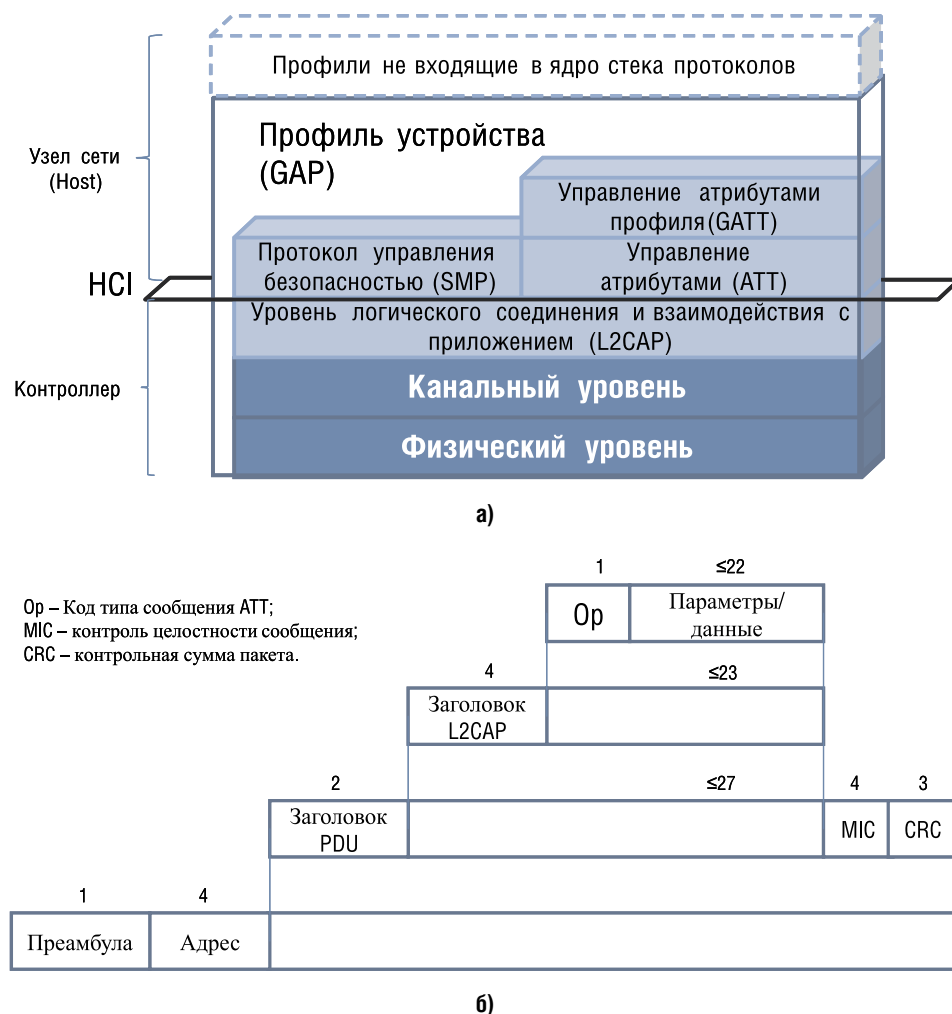


Рис. 1. Структура стека протоколов Bluetooth Low Energy (BLE) – а) и пакета данных BLE – б)

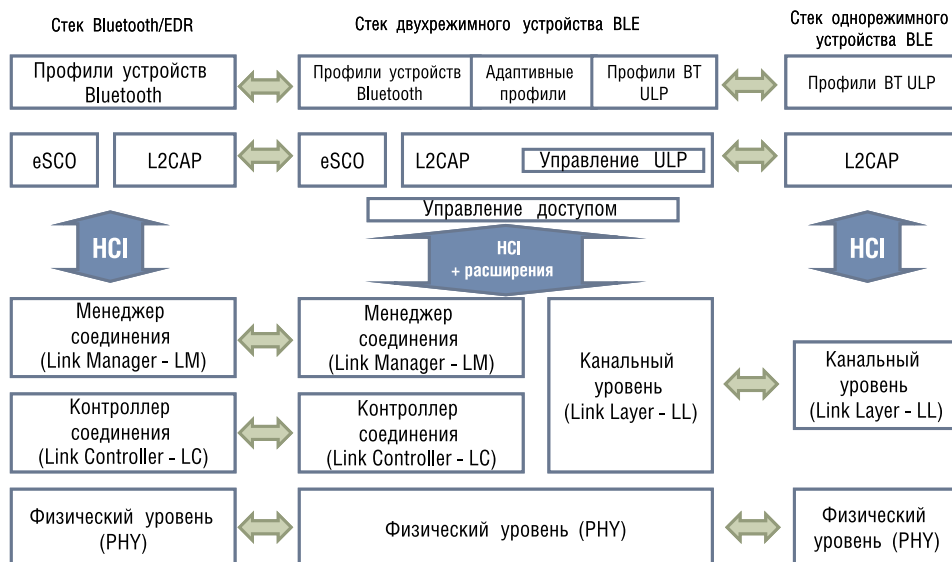


Рис. 2. Схема взаимодействия между однорежимными, двухрежимными устройствами и классическими Bluetooth-устройствами

ному компьютеру или информации, автоматическая блокировка-разблокировка системы в целях предотвращения несанкционированного доступа к информации, учет нахождения на рабочем месте (что полезно при внутреннем расследовании инцидентов, связанных с

нарушением политики информационной безопасности компании);

- в промышленном применении — автоматическая блокировка/разблокировка оборудования для защиты от несанкционированного включения (например, на время проведения ремонт-

ных или регламентных работ) или выключения;

- в строительной отрасли, при погрузочно-разгрузочных работах — для сигнализации нахождения в опасной зоне или индикации присутствия человека в зоне проведения работ.

Немаловажной областью применения BLE-устройств могут стать автомобильные системы. При помощи специальных BLE-брелоков или непосредственно со смартфона, оснащенного Bluetooth, возможно управление и настройка ряда автомобильных систем, начиная от личных настроек водителя (климат, предпочтительная радиостанция) до дополнительного уровня противоугонной системы. Таким уровнем может быть блокировка запуска автомобиля в отсутствии BLE-устройства (или любого из предварительно зарегистрированных устройств хозяина с Bluetooth) в радиусе действия BLE-узла, находящегося в автомобиле.

Ниже рассмотрим ключевые особенности стека протоколов Bluetooth Low Energy и BLE-устройств, поставляемых BlueGiga.

Стек протоколов Bluetooth Low Energy

Структура стека

Как и классический стек протоколов Bluetooth, стек BLE состоит из двух основных частей: контроллера (Controller) и узла сети (Host). Контроллер включает в себя физический и канальный уровень и часто реализуется в виде системы-на-кристалле (SoC) с интегрированным беспроводным трансивером. Часть стека, именуемая узлом сети реализуется программно на микроконтроллере приложений и включает в себя функциональность верхних уровней: уровень логической связи (Logical Link Control — LLC), протокол адаптации (Adaptation Protocol — L2CAP), протокол атрибутов (Attribute Protocol — ATT), протокол атрибутов профилей устройств (Generic Attribute Profile — GATT), протокол обеспечения безопасности (Security Manager Protocol — SMP), протокол обеспечения доступа к функциям профиля устройств (Generic Access Profile (GAP)). Взаимодействие между верхней и нижней частями стека осуществляется интерфейсом Host Controller Interface (HCI). Дополнительная функциональность прикладного уровня может быть реализована поверх уровня узла сети. На рисунке 1 представлена структура стека протоколов BLE [1, 3].

Несмотря на то, что некоторые функции контроллера BLE заимствованы у классического Bluetooth, они не совместимы между собой, т.е. устройство, поддерживающее только BLE (однорежимное устройство — single-mode

device) не сможет взаимодействовать с устройством, поддерживающим только Bluetooth 2.x/3.0. Для осуществления взаимодействия между ними хотя бы одно из устройств должно поддерживать оба стека протоколов (двухрежимное устройство – dual-mode device).

Однорежимные устройства обладают наименьшим потреблением и в основном представляют собой конечные исполнительные устройства. Двухрежимные устройства предполагают возможность периодического получения энергии, располагаются на различных мобильных устройствах, а также могут функционировать и как обычные Bluetooth-устройства. Схема взаимодействия между однорежимными, двухрежимными устройствами и классическими Bluetooth-устройствами представлена на рисунке 2 [1, 4].

Физический уровень

Устройства BLE работают в диапазоне 2,4 ГГц. В стандарте определено 40 частотных каналов с расстоянием в 2 МГц между каналами. На физическом уровне применена GFSK-модуляция (Gaussian Frequency Shift Keying) с индексом модуляции в пределах от 0,45 до 0,55, что позволяет уменьшить пиковое потребление энергии. Скорость передачи на физическом уровне 1 Мбит/с. В стандарте BLE чувствительность приемника определена как уровень сигнала на приемнике, при котором частота битовых ошибок (Bit Error Rate – BER) достигает уровня 10⁻³. Она должна составлять -70 дБм или лучше.

Выделяют два типа каналов – каналы объявления и каналы данных. Каналы объявления используются для поиска устройств, установления соединения, широковещательных передач, тогда как каналы данных используются для двустороннего обмена между устройствами.

Для каналов объявления выделено три частотных канала в центре полосы, что минимизирует перекрытие с каналами 1, 6 и 11 стандарта IEEE 802.11. Остальные 37 каналов используются для обмена данными. Для снижения влияния помех, многолучевого распространения, а также снижения влияния соседних устройств при обмене данными происходит скачкообразное переключение частоты (рис. 3) [1].

Канальный уровень

В BLE для передачи широковещательных пакетов применяются каналы объявления. Любое устройство, передающее пакеты по данным каналам, называется объявителем. Передача пакетов по каналам объявлений происходит только в течение специальных выделенных интервалов времени, называемых событиями объявлений. Во время этих

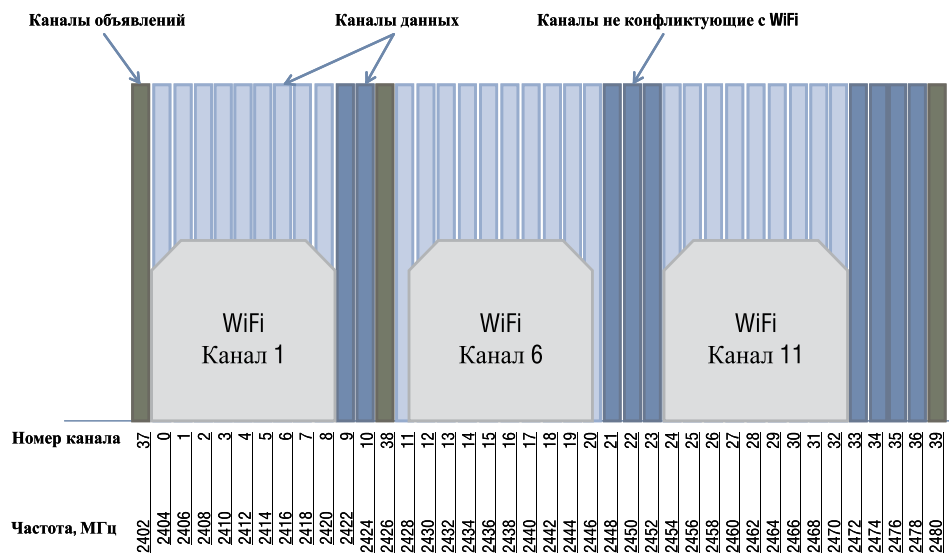


Рис. 3. Соотношение частотных каналов BLE и каналов IEEE 802.11

событий устройство-объявитель передает пакеты объявлений последовательно по каждому из трех каналов. Устройства, единственной функцией которых является прием пакетов объявлений, называются сканерами [3].

Двусторонний обмен между BLE-устройствами возможен только после установления соединения между ними. Создание нового соединения между двумя устройствами является асимметричной процедурой, в течение которой устройство-объявитель по каналам объявления сигнализирует о своей готовности к соединению, в то время как другое устройство (инициатор соединения) прослушивает данные каналы. Когда инициатор обнаруживает нужное устройство, он может послать запрос на установление соединения (Connection Request) объявителю, который устанавливает между ними соединение. С этого момента устройства могут осуществлять обмен по каналам данных. Пакеты, относящиеся к установленному соединению, будут отмечены сгенерированным случайным образом 32-битным кодом доступа.

Также как и в классическом варианте Bluetooth, в BLE для установления соединения одно из устройств выступает в качестве ведущего (master), второе – ведомого (slave). В ходе процедуры установления соединения – инициатор и объявитель, соответственно. Ведущее устройство может поддерживать несколько соединений с ведомыми, в то время как ведомое устройство может иметь только одно подключение – к ведущему. Таким образом, BLE-устройство одновременно может принадлежать только одной пико-сети. В этом кроется еще одно отличие BLE от Bluetooth – в последнем случае ведомое устройство в свою очередь могло выступать в качестве ведущего устройства своей собственной пико-сети.

Для экономии энергии ведомое устройство по умолчанию находится в спящем состоянии, периодически просыпаясь для проверки наличия пакетов данных от ведущего. Ведущий определяет для своих ведомых устройств моменты времени, в которые ведомый просыпается для прослушивания канала, регулируя тем самым доступ устройств к среде передачи по схеме разделения времени (Time Division Multiple Access – TDMA). Ведущее устройство также задает ведомым схему переключения частотных каналов. Параметры соединения передаются в сообщении запроса на установление соединения и могут быть обновлены при необходимости (например при смене схемы переключения каналов для устранения перекрытия с частотными каналами других устройств).

После установления соединения физический канал передачи данных разделяется на неперекрывающиеся временные интервалы, называемые событиями соединения (connection events) или фреймами. В течение фрейма все пакеты передаются по одному частотному каналу. Каждый фрейм начинается с передачи пакета ведущим устройством. В том случае, если ведомое устройство получило пакет, оно должно послать пакет-подтверждение. В то же время подтверждения от ведущего устройства ведомому не требуется. Между двумя последовательными пакетами должен быть выдержан интервал времени не менее 150 мкс – т.н. межкадровый интервал (Inter Frame Space – IFS).

До тех пор, пока между ведущим и ведомым продолжается обмен пакетами, событие соединения (или фрейм обмена) считается открытым. В пакетах данных, в случае необходимости дальнейшего обмена, установлен бит More Data (MD). Если ни одно из устройств не имеет данных для передачи, событие соединения

Таблица 1. Сервисы и уровни безопасности, определенные в стеке протоколов BLE [3]

Режим	Уровень безопасности	Тип соединения (Pairing)	Шифрование	Проверка целостности	Уровень стека
LE Security Mode 1	Уровень 1	Нет	Нет	Нет	Канальный уровень (Link Layer)
	Уровень 2	Без аутентификации	Есть	Есть	
	Уровень 3	Аутентификация	Есть	Есть	
LE Security Mode 2	Уровень 1	Без аутентификации	Нет	Есть	Уровень АТТ (ATT Layer)
	Уровень 2	Аутентификация	Есть	Есть	

будет закрыто, и ведомое устройство уже не должно прослушивать канал до начала следующего фрейма. Другими причинами, приводящими к закрытию события соединения, являются два последовательно принятых пакета с ошибками, неверный адрес устройства в пакете. Для контроля битовых ошибок в пакете после поля данных следует поле 24-битной контрольной суммы.

Для нового события соединения ведущий и ведомый используют новый частотный канал, заданный в карте переключения каналов. Время между началом двух последовательных событий соединения задается параметром *connInterval*, является кратным 1,25 мс и может лежать в пределах от 7,5 мс до 4 с. Вторым важным параметром для пико-сети BLE является параметр *connSlaveLatency*, определяющий количество последовательных фреймов, в течении которых ведомое устройство не прослушивает канал и может на это время отключить трансивер. Данный параметр является целым числом в пределах от 0 до 499, которое не должно превышать контрольного интервала супервизора — параметр *connSupervisionTimeout*. Параметр *connSupervisionTimeout* может принимать значения в диапазоне от 100 мс до 32 с. Его назначение — обнаружение потери соединения с устройством из-за ухудшения качества канала связи или перемещения его за пределы досягаемости [3].

На канальном уровне для управления потоком данных действует механизм остановки и ожидания (*stop-and-wait mechanism*) на основе т.н. кулюлятивного подтверждения, служащего одновременно и оповещением об ошибке. Заголовок каждого пакета, передаваемого по каналам данных, содержит два одноканальных поля, называемых порядковым номером и следующим ожидаемым порядковым номером (*Sequence Number (SN)* и *Next Expected Sequence Number (NESN)* соответственно). SN идентифицирует пакет, тогда как NESN показывает, какой пакет ожидается от устройства, с которым установлено соединение. Если пакет устройством принят успешно, поле NESN в его следующем пакете будет увеличено, и такой пакет одновременно будет считаться пакетом подтверждения. В противном случае,

если устройство обнаруживает ошибку (не сходится контрольная сумма), полю NESN в принятом пакете нельзя доверять, и устройство, принявшее такой пакет, повторяет отправку своего последнего пакета, что на стороне приемника в такой ситуации будет воспринято как сообщение об ошибке.

L2CAP

Протокол L2CAP в BLE является упрощенной и оптимизированной версией соответствующего протокола в Bluetooth 2.x/3.x. В BLE основной задачей L2CAP является мультиплексирование данных трех протоколов (ATT, SMP, Link Layer) для соединения канального уровня. Отвечает за установление логического соединения. Не производится сегментирования пакетов или сборки пакетов, т.к. максимальная полезная нагрузка L2CAP в BLE составляет 23 байта.

ATT

Определяет коммуникационные сообщения между двумя устройствами, выступающими в контексте данного протокола в качестве клиента и сервера.

Сервер поддерживает набор атрибутов, представляющих собой структуру данных, позволяющую получать доступ к информации, управляемой протоколом GATT. Роли клиента и сервера определяются протоколом GATT и не зависят от роли устройства в соединении (ведущий/ведомый).

Клиент посредством запросов может получить доступ к атрибутам сервера. Кроме того, сервер посылает клиенту два типа сообщений, содержащих атрибуты:

- уведомления, не требующие подтверждения;
- индикаторы, на которые клиент обязан ответить.

Клиент также может послать серверу команды на изменение значений атрибутов.

GATT

Протокол GATT определяет среду исполнения, используемую АТТ для обнаружения сервисов и обмена характеристиками между устройствами. Характеристика в данном случае представляет собой набор данных, включающих в

себя значения и свойства. Данные, относящиеся к сервисам и характеристикам, сохраняются в атрибутах.

К примеру, сервер с работающим сервисом «температурный датчик» может быть связан с характеристикой «температура», которая используется для описания датчика, а другой атрибут может применяться для хранения результатов измерений.

Вопросы безопасности BLE

BLE предлагает несколько сервисов безопасности для защиты данных, передаваемых между парой соединенных устройств. Большинство из поддерживаемых сервисов могут быть описаны в терминах двух режимов: LE Security Mode 1 и LE Security Mode 2. Эти режимы обеспечивают сервисы безопасности на канальном уровне и уровне АТТ, соответственно [3].

Канальный уровень BLE поддерживает шифрование и аутентификацию на основе алгоритма Cipher Block Chaining-Message Authentication Code (CCM) и блочного шифра AES-128. При использовании в соединении шифрования и аутентификации, к полезной нагрузке (PDU) добавляется четырехбайтное сообщение проверки целостности Message Integrity Check (MIC), после чего поля PDU и MIC шифруются.

Также возможна передача аутентификационных данных поверх нешифрованного соединения канального уровня. В данном случае на уровне АТТ к полезной нагрузке добавляется 12-байтная сигнатура. Сигнатура вычисляется путем использования алгоритма AES-128 как блочного шифра. Одним входом алгоритма является счетчик, позволяющий предотвратить атаки типа повтора сообщений. Если приемнику удастся верифицировать сообщение, считается, что оно пришло от достоверного источника.

В дополнение к описанным сервисам, BLE поддерживает механизм, называемый приватным (или частным) адресом, который позволяет устройству использовать множество часто меняемых адресов. Этот механизм снижает угрозу отслеживания BLE-устройства по его адресу. Приватные адреса генерируются на основе публичного адреса устройства путем его шифрования с

использованием ключа, полученного от доверенного устройства.

Каждый режим безопасности предусматривает наличие нескольких уровней, применяемых в зависимости от типа соединения пары устройств (таблица 1).

Логическое соединение устройств (pairing) происходит в три этапа. На первом этапе соединенные на канальном уровне устройства объявляют свои доступные возможности ввода-вывода, и на основе их принимается решение о методе взаимодействия на втором этапе.

Целью второго этапа является генерация короткоживущего ключа (Short-Term Key — STK), который будет использован на третьем этапе для обеспечения безопасности передачи распространения ключевой информации. На втором этапе устройства первоначально договариваются о временном ключе (Temporary Key — TK) при помощи одного из методов:

- Out Of Band;
- Passkey Entry;
- Just Works.

Метод Out Of Band (передача вне полосы) предполагает передачу временного ключа по альтернативным каналам, например, используя NFC. В методе Passkey Entry ключ задает пользователь в виде последовательности из шести цифр. Когда применение обоих методов невозможно, используется метод Just Work, хотя он не поддерживает проверку аутентификаций, и не защищен от атаки типа «посредник» (Man In The Middle — MITM).

На базе ключа TK и случайных чисел, генерируемых каждым из узлов, создается STK, что является завершением второго этапа.

На третьем этапе каждая из конечных точек соединения может передать другой конечной точке до трех 128-битных ключей, называемых Long-Term Key (LTK), Connection Signature Resolving Key (CSRK) и Identity Resolving Key (IRK).

LTK используется для генерации 128-битного ключа для шифрования и аутентификации на канальном уровне, CSRK — для подписи данных на уровне ATT, а IRK — для генерации частных адресов.

Протокол управления безопасностью Security Manager Protocol (SMP), работающий поверх фиксированного канала уровня L2CAP, отслеживает выполнение всех трех этапов.

Уязвимым местом BLE на текущий момент является незащищенность ни одного из реализованных в нем методов установления соединения от пассивного прослушивания. Однако, в следующих версиях BLE планируется использование эллиптической криптографической

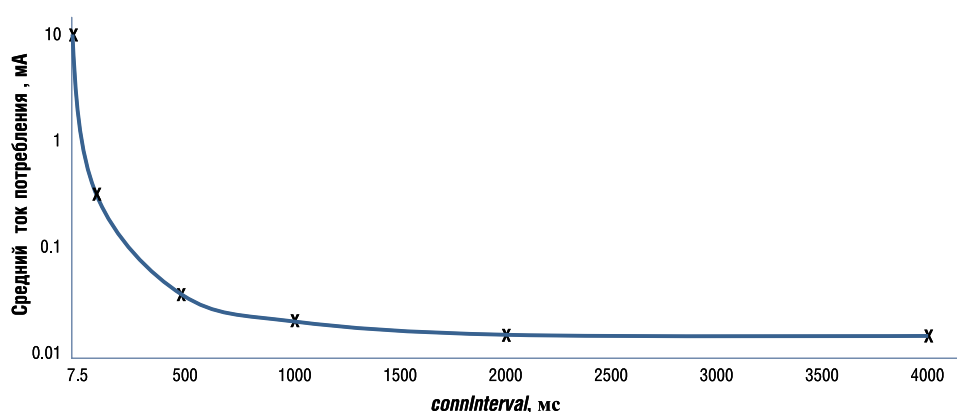


Рис. 4. Средний ток потребления BLE-устройства в режиме ведомого (узел построен на базе **СнК CC2450**, **connSlaveLatency=0**)

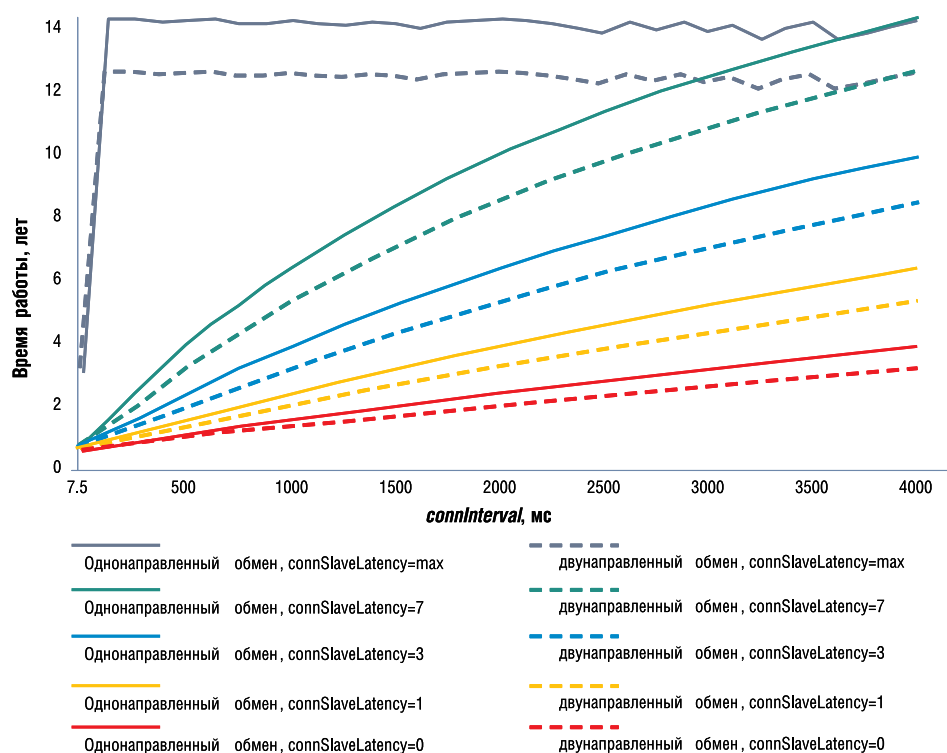


Рис. 5. Теоретические оценки времени автономной работы BLE-устройства на основе **CC2540** (от батареи емкостью **230 мАч** в режиме ведомого устройства при уровне ошибок равном 0 и максимальном значении **connSlaveLatency**)

кривой и алгоритма обмена открытыми ключами (алгоритм Диффи-Хелмана).

Уровень GATP и профили приложений

Протокол GATP определяет роли устройств, режимы и процедуры обнаружения устройств и сервисов, управление установлением соединения и безопасностью. В BLE GATP выделяет четыре роли для контроллера — широкопередаточный, наблюдатель, периферийный и центральный.

Широкопередаточный узел может только передавать пакеты по каналам объявления и не поддерживает соединение с другими устройствами. Наблюдатель способен только прослушивать каналы объявлений, в частности, способен принимать пакеты, передаваемые ши-

рокопередаточным узлом. Центральные узлы представляют собой устройства, способные поддерживать несколько соединений, в то время как периферийные — это простые устройства, способные поддерживать одно соединение с центральным узлом. Роли центрального и периферийного узла предполагают, что устройство способно выполнять функции, соответственно, ведущего или ведомого. Устройство может поддерживать несколько ролей, но одновременно активной может быть только одна из них.

Поверх GATP могут быть построены дополнительные профили приложений, обеспечивающие необходимую пользователю функциональность. В BLE поддерживается иерархия профилей — профиль

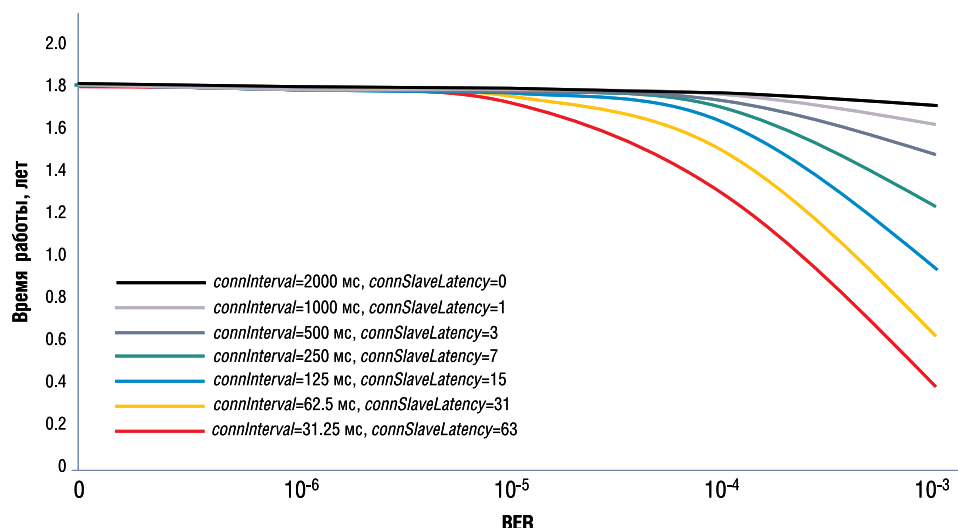


Рис. 6. Теоретические оценки времени автономной работы BLE-устройства на основе CC2540 (от батареи емкостью 230 мАч в режиме ведомого устройства при различном уровне ошибок и различных значениях параметров *connInterval* и *connSlaveLatency*)

верхнего уровня может использовать функции профиля низкого уровня.

Эксплуатационные характеристики BLE

Одним из важных показателей, определяющих возможность применения технологии беспроводной связи в той или иной задаче, является энергопотребление узлов сети, работающей по данной технологии. Этот показатель будет определять время автономной рабо-

ты устройств, и, соответственно, схему технического обслуживания сети.

Для устройств BLE потребление будет зависеть от роли устройства в соединении и параметрах соединения, в частности от *connInterval*, *connSlaveLatency*, *connSupervisionTimeout*, а также от качества связи.

Среднее энергопотребление узла в режиме ведомого в зависимости от величины *connInterval* представлено на рисунке 4 [3].

В [3] также представлены результаты теоретического анализа времени автономной работы BLE-устройства в качестве ведомого в зависимости от интервала следования событий связи *connInterval* и уровня битовых ошибок (BER) (рисунки 5 и 6, соответственно).

Данные результаты, хотя и представляют максимальные оценки времени работы BLE-устройств, но показывают, что BLE вполне подходит для сенсорных устройств с автономным питанием, и среднее потребление BLE-устройств вполне сравнимо с потреблением устройств, «традиционных» для сенсорных сетей.

Сравнительные характеристики технологий BLE, Bluetooth, ZigBee, 6LoWPAN, Z-Wave представлены в таблице 2 [1, 3].

Области применения BLE

Безусловно, большая часть областей применения Bluetooth может быть успешно заменена или дополнена устройствами BLE, что продлит срок службы устройств за счет более эффективного управления энергопотреблением. В частности, возможно применение двухрежимных устройств BLE в мобильных телефонах, планшетных компьютерах, ноутбуках. Однорежимные устройства могут применяться в качестве беспроводного интерфейса датчиков с батарейным питанием, применяющихся как отдельно, так и в составе других

Таблица 2. Некоторые сравнительные характеристики технологий BLE, Bluetooth, ZigBee, 6LoWPAN, Z-Wave

Параметр	ZigBee	6LoWPAN (поверх IEEE802.15.4)	Z-Wave	BLE	Bluetooth
Частотный диапазон, МГц	868/915/2400	—	868/908, 2400 (не все версии устройств)	2400	2400
Битовая скорость, кбит/с	20/40/250	—	9.6/40, 200	1000	<721 (v1.2), 3000(v2+EDR), <24000(v3+HS)
Тип модуляции сигнала	BPSK/BPSK/O-QPSK	—	BPSK	GFSK	GFSK(v1.2), GFSK/4-DQPSK/8DPSK (v2+EDR), 802.11 (v3+HS)
Метод расширения спектра	DSSS	—	Нет	FHSS (ширина канала 2 МГц)	FHSS (ширина канала 1 МГц)
Чувствительность приемника, дБм	-92 или лучше для 868/915 МГц; -85 или лучше для 2400 МГц	—	-101	<-70 -87...93	-90
Выходная мощность передатчика, дБм	-32...0	—	-20...0	-20...10	20/4/0 (класс 1/2/3)
Размер данных пакета, байт	До 127	—	До 64	От 8 до 47	До 358
Адресация	16- и 64-бит MAC, 16-бит идентификатор сети	16- и 64-бит MAC, 128-бит адрес IPv6	32-бит идентификатор дома; 8-бит адрес узла	48-бит открытый адрес Bluetooth или случайный адрес	48-бит открытый адрес Bluetooth
Типовые требования к реализации стека протоколов	45...128 кбайт ПЗУ; 2,7...12 кбайт ОЗУ	~24 кбайт ПЗУ; ~3,6 кбайт ОЗУ	32...64 кбайт ПЗУ; 2...16 кбайт ОЗУ	~40 кбайт ПЗУ; ~2,5 кбайт ОЗУ	~100 кбайт ПЗУ; ~30 кбайт ОЗУ



Рис. 7. Внешний вид двухрежимного BLE-модуля BT111

устройств — в часах, пульсометрах, шагомерах, домашних тонометрах, термометрах и тому подобных устройств.

В составе мобильных устройств BLE может быть использован для управления домашней автоматикой, устройствами освещения или охраны, как минимум, в пределах одного помещения. Для управления устройствами в пределах всего дома возможно использование BLE в качестве шлюза между управляющим устройством и сетью домашней автоматикой.

Низкое энергопотребление и более устойчивая работа в условиях большого количества аналогичных устройств в ряде случаев позволяет рассматривать BLE как альтернативу устройствам NFC, в частности RFID-меткам. Но более интересен вариант использования BLE совместно с NFC. В этом случае первые обеспечивают больший радиус устойчивой работы и большое количество совместно работающих устройств, а вторые служат для установления логического соединения между парой устройств, обеспечивая более высокий уровень безопасности за счет меньшего радиуса действия.

Модули Bluetooth Low Energy компании BlueGiga

На данный момент BlueGiga предлагает серии BLE-устройств [5, 6]:

- модуль **BT111** Bluetooth Smart Ready HCI Module;
- USB-устройство **BLED112** Bluetooth low dongle;
- модуль **BLE112** Bluetooth low energy module.

Модуль BT111

BT111 предназначен для приложений, в которых необходима работа и с классическими Bluetooth-устройствами, и с устройствами Bluetooth Low Energy, и представляет собой миниатюрный модуль поверхностного монтажа со встроенной антенной (рис. 7).

При выходной мощности до 8 дБм модули BT111 могут поддерживать соединение на расстоянии порядка 100 м в пределах прямой видимости. Чувствительность приемника составляет -89 дБм.

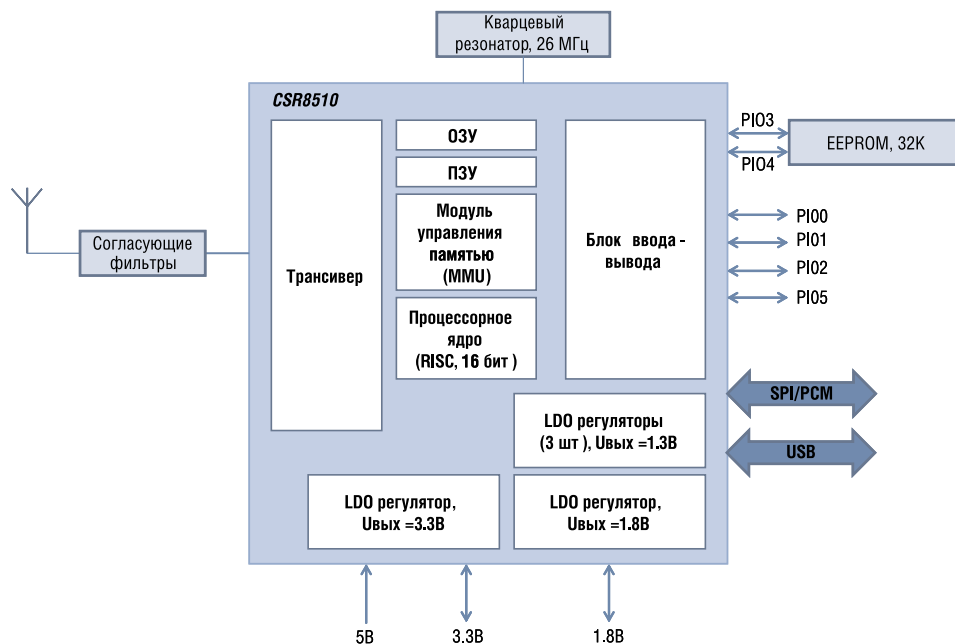


Рис. 8. Структурная схема BLE модуля BT111

В основе BT111 лежит беспроводная система-на-кристалле CS8510 [7], содержащая Bluetooth-трансивер, 16-битный RISC-микроконтроллер с достаточно эффективной схемой управления энергопотреблением и распределением памяти. Ядро микроконтроллера при поддержке контроллера прерываний и таймера исполняет стек протоколов Bluetooth, а также отслеживает беспроводной интерфейс и интерфейс к хост-контроллеру. Встроенный в CS8510 LDO-регулятор позволяет модулю работать в диапазоне напряжений от 1,8 до 3,6 В.

CS8510 дополнительно имеет SPI-, PCM- и USB (Full-speed 12 Мбит/с)-интерфейсы. Кроме того, доступны до четырех линий ввода-вывода, которые могут быть использованы в качестве линий индикаторов, в качестве входных линий, а также в режиме совместимости с Wi-Fi.

Помимо самой однокристалльной системы CS8510 в состав BT111 входят: монополярная керамическая антенна, входной фильтр, EEPROM объемом 32 кбайта и кварцевый резонатор на 26 МГц. Структурная схема BT111 представлена на рисунке 8.

Антенна обеспечивает усиление порядка 0,5 дБм, радиочастотный фильтр позволяет уменьшать уровень помех модуля. Встроенная EEPROM может быть использована для хранения настроек модуля, таких как выходная мощность передатчика, конфигурация периферийных интерфейсов, настройки и идентификаторы USB, адрес Bluetooth.

BT111 может работать совместно с Wi-Fi-устройствами. Для этого предусмотрено три режима совместимости:

- Unity-3;
- Unity-3e;
- Unity+.

CS8510 обладает весьма впечатляющими объемами памяти и эффективной схемой управления ею. Так, модуль управления памятью поддерживает несколько кольцевых буферов для передачи данных между хост-контроллером и беспроводным интерфейсом при минимальном участии в этом процессорного ядра.

В CS8510 56 кбайт оперативной памяти разделяется между кольцевыми буферами для голосовых данных или для пакетов данных для каждого из поддерживаемых активных соединений. Встроенная постоянная память объемом 5 Мбайт предназначена для хранения прошивки стека протоколов, настроек модуля и кода прикладных программ.

Модуль BLE112

Модуль **BLE112** (рис. 9) является однорежимным BLE-модулем, предназначенным для сенсорных систем и BLE-аксессуаров с батарейным питанием. BLE112 поддерживает практически все возможности устройств BLE — беспроводная передача данных, поддержка стека протоколов BLE и ряда профилей BLE-устройств, дополнительно присутствует возможность хранения пользовательских приложений. Таким образом,



Рис. 9. Внешний вид модуля BLE112

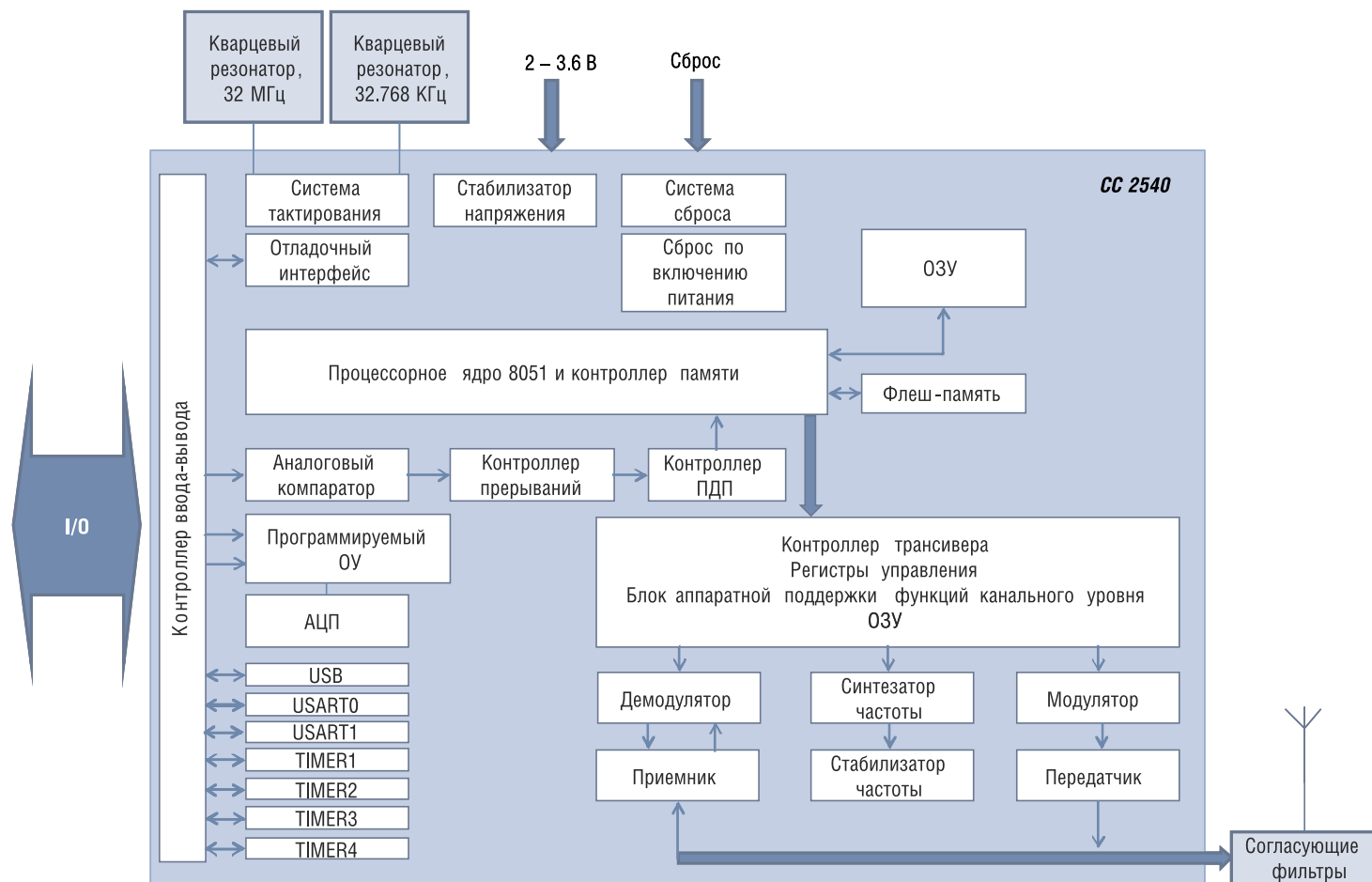


Рис. 10. Структурная схема модуля BLE112

возможна работа модуля BLE без внешнего контроллера.

BLE112 отличается достаточно низким энергопотреблением и широким диапазоном напряжений питания. Так он может напрямую работать от 3 В батарейки типа «монета» или от пары батареек типа AAA. В режиме сна модуль потребляет только порядка 400 нА, переход в активный режим осуществляется за доли миллисекунд, а в режиме передачи ток потребления составляет около 27 мА (при выходной мощности 0 дБм).

Трансивер BLE112 обеспечивает выходную мощность в пределах от -23 до 3 дБм и чувствительность по приему порядка -85...-91 дБм.

BLE112 основан на BLE-процессоре от Texas Instruments CC2540 [8], и в дополнение к самому беспроводному

процессору имеет встроенные кварцевые резонаторы на 32 МГц и на 32,678 КГц, обеспечивающие тактирование CC2540, согласующий фильтр и миниатюрную керамическую антенну. На печатной плате модуля предусмотрено также посадочное место для

UFL-разъема, позволяющего подключать внешнюю антенну.

Структурная схема BLE112 представлена на рисунке 10.

CC2540 содержит высокопроизводительный микроконтроллер архитектуры 8051 с 8 кбайт оперативной памяти и



Рис. 11. Внешний вид USB-BLE модуля BLE112

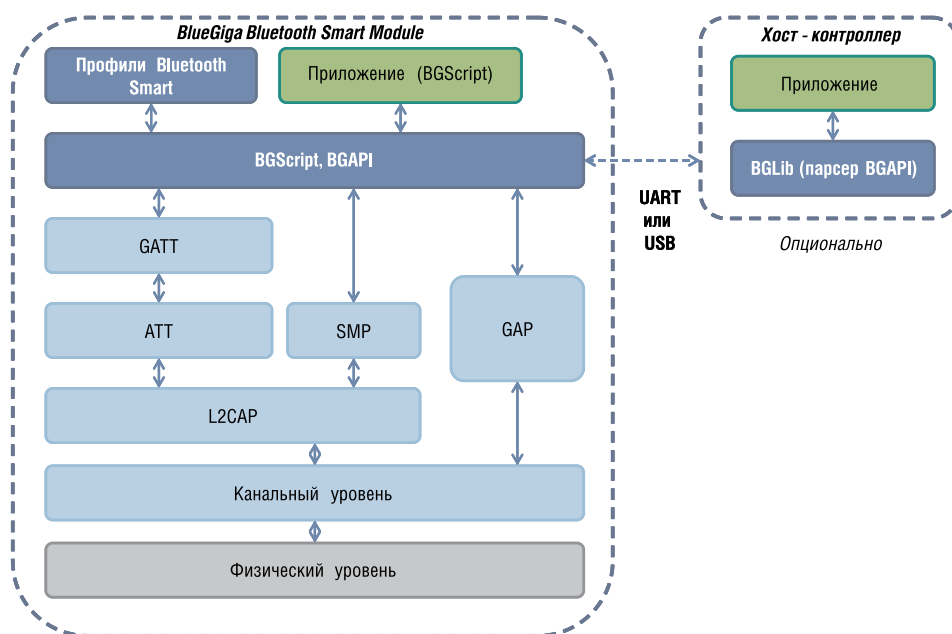


Рис. 12. Структурная схема программного обеспечения, предоставляемого BlueGiga

до 256 кбайт флеш-памяти с возможностью перепрограммирования самим устройством. Пятиканальный контроллер прямого доступа в память позволяет весьма эффективно организовать работу с периферийными устройствами и памятью, существенно экономя ресурсы процессорного ядра. Контроллер прерываний обслуживает до 18 каналов прерываний с четырьмя уровнями приоритета, включая прерывания от таймеров, периферийных устройств, линий ввода-вывода.

Набор периферийных устройств включает в себя:

- таймер с ультранизким потреблением, работающий от внешнего 32 кГц резонатора;
- сторожевой таймер;
- 40-битный таймер, используемый стеком протоколов BLE;
- 16-битный таймер с функциями счетчика, ШИМ-генератора и таймера;
- два 8-битных многофункциональных таймера (таймер/счетчик/ШИМ);
- два асинхронных последовательных интерфейса;
- модуль шифрования (AES128);
- 8-канальный АЦП с разрядностью от 7 до 12 бит и скоростями преобразования от 30 до 4 кГц и встроенным датчиком температуры;
- аналоговый компаратор.

Еще одним устройством, предлагаемым BlueGiga для приложений BLE, является USB-BLE модуль **BLED112** (рис. 12). Сохраняя функциональность, аналогичную модулю **BLE112** (за исключением возможностей ввода-вывода), он выполнен в формате USB-устройства и позволяет подключать другие BLE к персональному компьютеру. **BLED112** может также выполнять роль виртуального COM-порта или USB-HID устройства.

BLED112 может также быть полезен при отладке и демонстрации приложений, использующих стек протоколов Bluetooth Low Energy.

Программное обеспечение

BlueGiga предоставляет ряд инструментов и сред для разработки BLE-приложений, а также для настройки модулей и отладки встроенного программного обеспечения.

Программный интерфейс **BGAPI™** совместно с библиотекой **BGLib™ C-library** позволяет достаточно легко и эффективно использовать ресурсы модулей BlueGiga при помощи внешнего хост-контроллера (рис. 12).

Программный пакет Profile Toolkit™ позволяет производить разработку и отладку пользовательских приложений для BLE-модулей.

BGScript™ предназначен для быстрой разработки приложений без глубоких знаний особенностей работы

стека протоколов, для отладки и тестирования логики работы приложений. Приложения на BGScript™ могут разрабатываться и для хост-контроллера и для самих модулей.

Заключение

Технология Bluetooth Low Energy представляется весьма перспективной технологией для сенсорных приложений, особенно связанных с тесным взаимодействием с пользователем. BLE имеет большой потенциал для широкого распространения, связанный в том числе с успехом классического Bluetooth.

Специализирующаяся на Bluetooth-устройствах компания BlueGiga выпускает одно- и двухрежимные устройства BLE, включая модули поверхностного монтажа и USB-устройства, позволяющие благодаря компактным размерам и низкому энергопотреблению реализовывать приложения практически любых областей применения технологии BLE.

Литература

1. Bluetooth® low energy technology// http://www.compel.ru/wordpress/wp-content/uploads/2012/04/Bluetooth_low_energy_technology.pdf
2. Johanna Nieminen. Connecting IPv6 capable Bluetooth Low Energy sensors

with the Internet of Things//http://www.futureinternet.fi/seminar2012/Nieminen_IPv6_over_BTLE_300512.pdf

3. Carles Gomez, Joaquim Oller and Josep Paradells. Overview and Evaluation of Bluetooth Low Energy: An Emerging Low-Power Wireless Technology. <http://www.mdpi.com/1424-8220/12/9/11734>

4. Flavia Martelli. Bluetooth® low energy. http://www.chiaraburatti.org/uploads/teaching/handouts_WSNs_BT-LE.pdf

5. Bluegiga — Bluetooth_Modules// <http://www.bluegiga.com/bluetooth-low-energy>

6. Виктор Алексеев. Новые модули Bluetooth 4.0 серии BLE производства Bluegiga.//Беспроводные технологии. 2011. №2. С. 16 – 22.

7. CSR8000™ Platform//<http://www.csr.com/products/54/csr8000-platform>

8. 2.4GHz Bluetooth® low energy System-on-Chip//<http://www.ti.com/lit/gpn/cc2540>.

Получение технической информации,
заказ образцов, поставка –
e-mail: wireless.vesti@compel.ru



bluegiga
Bluetooth SMART

BLE112
Bluetooth-модуль
SMART Energy
Bluetooth v 4.0

- Bluetooth v4.0, режим «single mode»
Поддерживается режим «master» и «slave»
- Интегрированный стек протоколов
Bluetooth low energy
GAP, GATT, L2CAP и SMP. Профили Bluetooth Smart
- Радиочастотные характеристики:
-Выходная мощность: +3...-23 дБм
-Чувствительность: -87...-93 дБм
- Ультранизкое потребление
Передача: 27 мА (0 дБм). Сон: 0.4 мкА

0 cm

Москва
Тел.: (495) 995-0901, доб. 2387
Шевелев Сергей
E-mail: s.shevelev@compel.ru

Санкт-Петербург
Тел.: (812) 327-94-04, доб. 4231
Романов Олег
E-mail: Romanov.spb@compel.ru

Компэл
www.compel.ru

Андрей Никитин (г. Минск)

ДЛЯ ЗАМЕНЫ «ТАБЛЕТОК»: СИСТЕМЫ РЧ-ИДЕНТИФИКАЦИИ НА БАЗЕ КОМПОНЕНТОВ RFID КОМПАНИИ MAXIM INTEGRATED



В статье рассматриваются новые **RFID-компоненты Maxim**: изделия **MAX66040** и **MAX66140**, в которых реализован алгоритм **криптографического хеширования SHA-1**, и отладочные наборы, предлагаемые производителем для упрощения разработки систем контроля доступа.



Система контроля доступа (СКД) — комплекс аппаратно-программных средств безопасности, предназначенный для контроля (ограничения, регистрации) входа-выхода людей и/или транспортных средств на определенные территории через так называемые «точки прохода» (двери, ворота, проходные). Кроме того, задачами СКД могут быть также учет рабочего времени персонала и контроль прав доступа работающих к конкретному оборудованию компании (компьютеры, ксероксы, принтеры).

Ключевыми элементами любой СКД являются идентификатор и считыватель. Идентификатор (ключ) — это то, что хранит некий код, служащий для идентификации владельца и, следовательно, определяющий права его предъявителя. Считыватель — устройство, которое этот код считывает. Строго говоря, идентификатором может являться и сам человек. Существуют достаточно надежные системы доступа, основанные на биометрической идентификации. Это, например, анализ отпечатка пальца, анализ радужной оболочки или сетчатки глаза субъекта. Однако, системы, основанные на биометрической идентификации, имеют в настоящее время еще довольно ограниченное применение. Поэтому в качестве идентификатора в большинстве систем используется предмет, принципиально небольшого веса и габаритов, хранящий некий код, используемый для принятия решения о разрешении доступа. Отметим, что идентификаторы-устройства являются пропуском «на предъявителя», то есть они никаким образом не гарантируют, что идентификатор предъявит для доступа именно его законный владелец, а не постороннее лицо, владеющее «пропуском» в данный момент времени.

Наиболее распространенные устройства, выполняющие функции идентификатора:

1. Магнитные карты или карты с магнитной полосой. Позволяют считывать и записывать ограниченный объем информации. Надежность и защищенность магнитных карт в настоящее время оценивается как недопустимо низкая. В новых разработках эти карты практически не применяются, хотя в старых, масштабных проектах используются до сих пор. Например, в некоторых городах магнитные карты продолжают использоваться как проездные билеты в метрополитене.

2. Контактная память или «таблетка». В различных публикациях называется также Touch Memory или iButton. Это электронные компоненты с однопроводным протоколом обмена информацией (1-Wire), размещенные в стандартном металлическом корпусе (действительно похожем на таблетку). В наиболее простом варианте электронного ключа при считывании выдавался длинный номер, записываемый в устройство при изготов-

лении. Более сложные варианты изделий содержали энергонезависимую перезаписываемую память, контроллеры, таймеры, датчики температуры. Обмен данными производился при контакте со специальными считывателями, причем сама «таблетка» активизировалась для чтения-записи только в момент контакта. В странах бывшего СССР появились в самом начале 90-х годов, но и в настоящее время продолжают широко использоваться в бюджетных приложениях. Например, как ключи к домофонам в подъездах жилых домов.

3. Контактные смарт-карты представляют собой пластиковую карту со встроенной микросхемой (часто микропроцессор средней вычислительной мощности). С функциональной точки зрения — аналог «таблеток». Различия заключается исключительно в конструктивном исполнении. Контактные смарт-карты имеют небольшую зону, содержащую несколько металлических

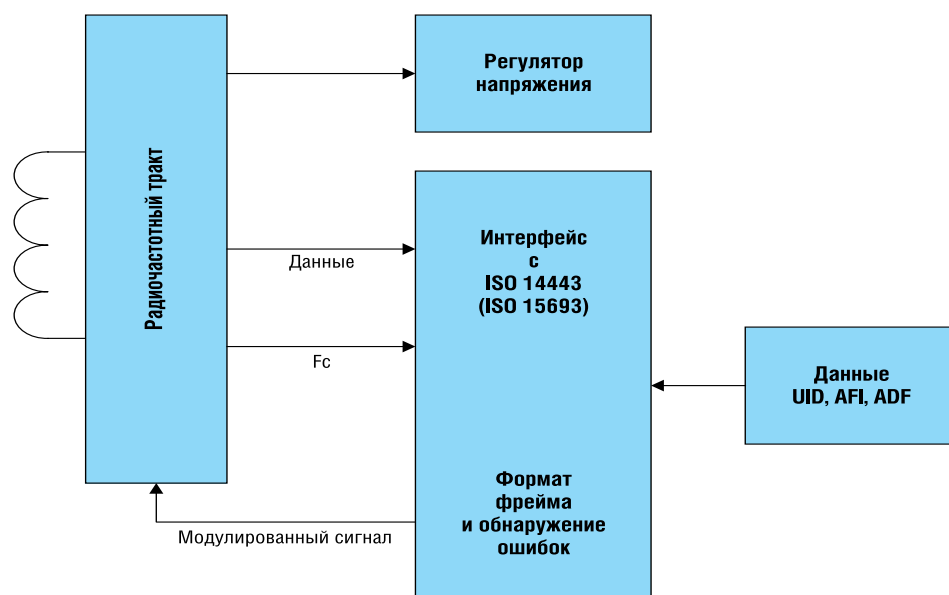


Рис. 1. Структурная схема идентификаторов MAX66000 и MAX66100

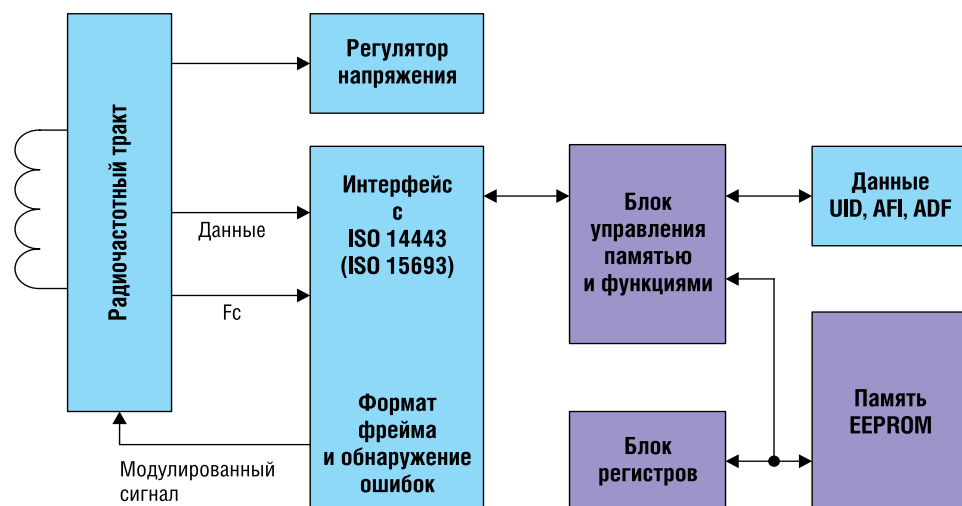


Рис. 2. Структурная схема идентификаторов MAX66020 и MAX66120

контактных лепестков. Когда карта вставлена в считыватель, то чип карты соприкасается с электрическими контактами считывателя, и последний получает доступ к информации с чипа. Вычислительная мощность микропроцессора позволяет не только считать и записать данные в энергонезависимую память, но, в ряде приложений, поддерживать выполнение специфических криптографических функций. Основная сфера применения: банковские карты, проездные билеты, второстепенные документы (например, студенческие и читательские билеты), ключи для систем доступа.

4. Бесконтактные смарт-карты — это смарт-карты, использующие технологию RFID (*Radio Frequency IDentification*). Для проведения необходимых операций требуется поднести карточку достаточно близко к считывателю. Однако непосредственное касание не требуется, так как обмен данными происходит по радиоканалу. Бесконтактные смарт-карты подразделяются на два класса: так называемый proximity card, соответствующий стандарту ISO/IEC 14443 и vicinity card, соответствующий стандарту ISO/IEC 15693. Основное отличие: в первом случае расстояние от карты до считывателя не превышает 15 сантиметров, а во втором увеличено до 100 сантиметров. То есть, в первом случае карту следует все же поднести к считывателю достаточно близко, а во втором она может оставаться в кармане пальто. Рабочая частота в обоих случаях составляет 13,56 МГц, однако скорости обмена данными в первом случае заметно выше: 106...848 кбит/с против 1,6...26 кбит/с.

Считается, что бесконтактные карты по сравнению с контактными ключами имеют существенный плюс: такую карту не требуется вставлять в считыватель — достаточно поддержать ее в непосредственной близости от него. Предполагается, что такой способ повышает

пропускную способность «точки прохода». Но применительно к СКД это, скорее всего, несущественно: если алгоритм допуска на режимную территорию (помещение) предполагает проход через турникет по одному человеку, то пропускная способность будет определяться именно турникетом. Реальный выигрыш будет в других факторах. Во-первых, отсутствие механических частей и контактов существенно повышает срок работы и самих ключей, и считывателей. Во-вторых, подделка бесконтактной карты, в принципе, возможна, но трудозатраты на эту процедуру будут на порядок выше, чем при использовании «таблетки» или контактной смарт-карты. Фактор стоимости в настоящее время не представляется существенным: разница в цене контактного и бесконтактного исполнений скажется только в СКД с числом пропусков от десятков тысяч и более.

Алгоритмы защиты информации

Рекомендуемые к применению в новых разработках RFID-ключи компании Maxim предполагают наличие встроенного блока, реализующего алгоритм SHA-1 (*Secure Hash Algorithm*) — алгоритм криптографического хеширования, то есть вычисления хеш-суммы — значения какой-то конкретной для данного алгоритма хеш-функции, вычисленной на принятой последовательности данных. Для входного сообщения произвольной длины алгоритм SHA-1 генерирует 160-битную хеш-сумму, которая также называется дайджестом. Строго говоря, любая контрольная сумма, например, CRC32, которая используется во многих программах — это тот же дайджест, только вычисленный по другому алгоритму. В криптографии применяемая хеш-функция должна удовлетворять трем требованиям. Во-первых, необра- тимость, то есть по дайджесту долж-

но быть невозможным восстановить входное сообщение. Во-вторых, по заданному дайджесту должно быть вычислительно невозможно (то есть, невозможно за разумное время) подобрать сообщение, которое будет иметь этот же дайджест. В-третьих, по исходному сообщению вычислительно невозможно подобрать другое сообщение, имеющее аналогичный дайджест.

Что на практике дает применение алгоритма криптографического хеширования? Если криптографическая защита в СКД не используется, то для того, чтобы инициировать некую операцию (например, открыть дверь в помещение) с карты-идентификатора клиента, необходимо отослать на сервер некоторый код, выполняющий функцию пароля. Сервер сравнит полученный пароль со списком допустимых вариантов и, если в этом списке найдется полученный пароль, разрешит доступ к запрошенной операции. Заполучив каким-то образом этот список, злоумышленник может симитировать отсылку требуемого пароля и получить право на доступ. При использовании криптографической защиты на сервере хранятся не сами пароли, а только их дайджесты. В этом случае ситуация для злоумышленника становится практически неразрешимой. Чтобы получить доступ, надо отослать пароль, но сервер хранит не пароли, а дайджесты от пароля и, только получив сообщение-пароль, рассчитывает дайджест. Причем само принятое сообщение на сервере принципиально не запоминается. Если полученный дайджест есть в списке разрешенных, то сервер дает право на запрашиваемую операцию. Злоумышленник, получив доступ к серверу, может узнать только разрешенные дайджесты, но не сам список паролей. А зная только дайджест, он не может за разумное время подобрать допустимый пароль и, таким образом, даже обладание файлом дайджестов не дает возможность получить право на требуемую операцию. Примерно аналогичным образом процессор на карте клиента может проверять право сервера изменить (записать) некую информацию в свою пользовательскую и системную память (когда это возможно в принципе).

Иными словами, речь идет не о шифровании или дешифровании самих передаваемых сообщений — предполагается, что злоумышленник не имеет возможность «прослушивать» канал обмена. Если это не так, то теряется смысл применения алгоритмов криптозащиты. Речь идет только лишь о невозможности за разумное время подобрать допустимые сообщения-пароли, имея в распоряжении список разрешенных дайджестов. Отметим, однако, что алгоритм SHA-1 не является какой-то обязательной или даже желательной частью стандарта на

бесконтактные карты. Существует, как минимум, десятка два алгоритмов, подобных SHA-1, разной степени популярности, которые различаются конкретной процедурой формирования дайджеста и теоретически оцененным временем подбора входного сообщения с заданным дайджестом (причем во всех случаях избыточным). Все обязательные требования к бесконтактным proximity- (или vicinity-) картам определяются стандартами ISO/IEC 14443B (или ISO/IEC 15693) и только ими. Все остальное, в частности — алгоритмы хеширования, является надстройкой, которая может присутствовать, а может и отсутствовать в конкретном приложении.

Бесконтактные идентификационные карты компании Maxim

В настоящее время компания Maxim в линейке RFID-компонентов для идентификации предлагает два изделия: **MAX66040** и **MAX66140**. Первое — MAX66040 — поддерживает стандарт ISO/IEC 14443B, и, соответственно, предназначено для приложений направления proximity card. Второе — MAX66140 — поддерживает ISO/IEC 15693 и приложения vicinity card. Имеет смысл начать рассмотрение с ранних изделий для понимания развития направления RFID-идентификаторов, предлагаемых компанией Maxim (в настоящее время не рекомендуются для новых разработок).

Простейшие идентификаторы **MAX66000** и **MAX66100** включали в себя 64-разрядный уникальный номер изделия (UID), задаваемый в процессе изготовления, и радиочастотный интерфейс 13,56 МГц, удовлетворяющий требованиям ISO/IEC 14443B или ISO/IEC 15693 (для MAX66000 и MAX66100 соответственно). Структурная схема идентификаторов **MAX66x00** представлена на рисунке 1. Данные устройства поддерживали только две команды управления: «Get System Information» (чтение системной информации) и «Get UID» (чтение UID).

Усовершенствованием этих изделий были идентификаторы **MAX66020** и **MAX66120**, которые также включали в себя 64-разрядный уникальный номер изделия и радиочастотный интерфейс 13,56 МГц (также в двух вариантах реализации). Дополнительно изделия содержали пользовательскую память EEPROM (электрически стираемое, программируемое пользователем ПЗУ) объемом 1024 бита, организованную как 16 блоков по 8 байт. Кроме того, в пространство памяти входило два дополнительных блока для организации регистров данных и управления.

Структурная схема идентификаторов **MAX66x20** представлена на рисунке 2. Фиолетовым цветом выделены блоки,

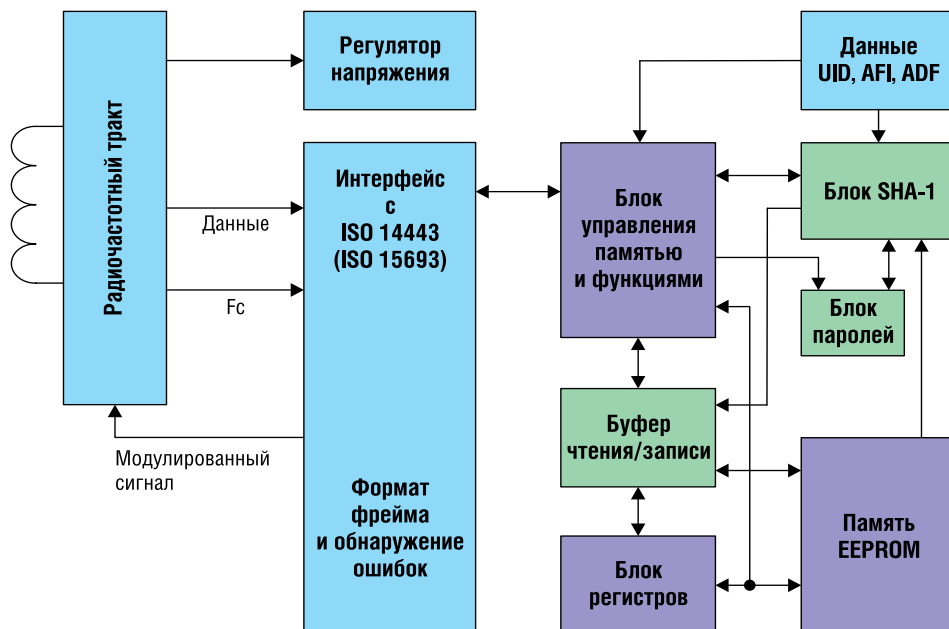


Рис. 3. Структурная схема идентификаторов MAX66040 и MAX66140

отсутствующие в изделиях MAX66x00. Изделия MAX66x20 могли быть использованы как прямая замена ключей MAX66x00, поскольку форматы команд управления «Get System Information» и «Get UID» были сохранены без каких либо изменений. Однако, дополнительно были добавлены команды, поддерживающие чтение отдельного блока памяти, запись в блок и его закрытие. Расширенные команды позволили содержать на карте не только постоянную информацию, записанную при изготовлении, но и небольшой объем пользовательских данных (например, ФИО и должность владельца, структурное подразделение и т.п.).

Идентификаторы MAX66040 и MAX66140 являются дальнейшим развитием этого направления. Эти изделия, как и их предшественники, включают в себя 64-разрядный уникальный номер изделия и радиочастотный интерфейс. Пользовательское EEPROM имеет объем 1024 бита, организацию «16 блоков по 8 байт» и два дополнительных блока, что соответствует архитектуре памяти изделий MAX66x20. Команды управления памятью, присутствующие в изделии MAX66x20, сохранены в идентификаторах MAX66x40 без изменений. Таким образом обеспечивается совместимость изделий MAX66x40 с более ранними компонентами MAX66x20 и, соответственно, MAX66x00. То есть, идентификаторы MAX66x40 могут быть использованы как прямая замена MAX66x20 и MAX66x00 без внесения каких-либо изменений в само приложение. Однако, в дополнение к MAX66x20, изделия MAX66x40 имеют третий дополнительный блок, предназначенный для хранения пароля, а также встроенный блок, аппаратно реализующий защиту

на базе алгоритма хеширования SHA-1. Система команд расширена таким образом, что позволяет изделию работать как без использования средств защиты SHA-1 (то есть, в режиме MAX66x20), так и реализует возможности MAX66x40 в полном объеме. Структурная схема идентификаторов MAX66x40 представлена на рисунке 3. Светло-зеленым цветом выделены новые, по сравнению с MAX66x00 и MAX66x20, блоки. Введение дополнительных средств криптографической защиты позволило значительно расширить возможную сферу применения RFID-ключей компании Maxim до современных СКД с серьезными требованиями к безопасности и защите от несанкционированных воздействий.

Отметим, что изделия MAX66x40 выпускаются в виде двух возможных форм-факторов. Исполнение в виде бесконтактной смарт-карты стандартных размеров имеет суффикс «Е» (например, **MAX66040E**), а исполнение в виде брелка — суффикс «К».

Несколько слов о карт-ридерах, предназначенных для работы с RFID-идентификаторами MAX66xx0. Эту продукцию разного качества выпускают многие независимые компании. Для работы с идентификаторами **MAX660x0** (**MAX661x0**) достаточным требованием является соответствие карт-ридера стандарту ISO/IEC 14443B (или ISO/IEC 15693, соответственно). То есть на «стандартном» карт-ридере можно гарантированно считать с карты ее UID. Для карт с EEPROM должны быть задействованы функции доступа к другим ресурсам карты, которые оговорены в части 4 стандарта ISO/IEC 14443B, где определяется протокол обмена данными. Однако эта часть реализована далеко не



Рис. 4. Состав отладочного комплекта MAX66901 EV Kit

в любом карт-ридере, соответствующем ISO/IEC 14443B. Если в приложении необходим доступ к другим ресурсам карты (к той же памяти), то необходимо убедиться, что карт-ридер «понимает» именно ISO/IEC 14443B-4. Для стандарта ISO/IEC 15693 ситуация аналогична, с той лишь разницей, что протокол обмена данными регламентирован третьей частью этого стандарта — ISO/IEC 15693-3. Функции криптозащиты, заложенные в MAX66x40, в настоящее время непосредственно карт-ридерами не поддерживаются, а реализуются поверх стандартов ISO/IEC 14443B (ISO/IEC 15693) на уровне программного обеспечения сервера.

Отладочные комплекты для работы с RFID-идентификаторами компании Maxim

Основным отладочным комплектом, предлагаемым компанией Maxim для работы с RFID-ключами MAX660x0 и MAX661x0, является **MAX66901 EV Kit**. В комплект входит карт-ридер **INfinity-110** американской компании **Sirit** с соответствующим программным обеспечением, источник питания, необходимые кабели и переходники, а также RFID-брелки MAX660xxK (всех шести типов ключей, выпускаемых компанией Maxim). Непосредственно карт-ридер INfinity-110 поддерживает работу с картами стандартов ISO/IEC 14443B и ISO/IEC 15693 в полном объеме, то есть позволяет считывать UID устройств, обеспечивает возможность работы со всем пространством памяти ключей MAX66x20 и MAX66x40 и работу с функциями криптозащиты SHA-1, которые реализованы в MAX66x40. Отладочный комплект позволяет выполнить следующие процедуры работы

с пространством памяти: чтение системной информации, чтение UID, чтение, запись и закрытие блоков памяти, запись и закрытие байта AFI. В режиме работы с использованием функций SHA-1 комплект позволяет записать блок паролей, произвести чтение-запись в блок дайджестов, выполнить расчет дайджеста и провести проверку аутентификации. Отметим, что программное обеспечение, входящее в состав отладочного комплекта, несколько отличается от фирменного ПО, поставляемого компанией Sirit с модулем INfinity-110. Программа для работы с комплектом MAX66901 EV Kit не содержит операций для работы с RFID-ключами тех типов, которые не входят в номенклатуру компании Maxim (например, ключи **Mifare** компании **NXP**), что позволяет в наибольшей степени сконцентрироваться на особенностях именно изделий Maxim. Фотография отладочного комплекта MAX66901 EV Kit представлена на рисунке 4. Для работы только с изделиями MAX661x0 (категория vicinity card) существует также отладочный комплект MAX66903 EV Kit. Однако существенных дополнительных возможностей (по сравнению с MAX66901 EV Kit) он не предоставляет.

Отличительные особенности RFID-идентификаторов MAX66x40 компании Maxim

Бесконтактные ключи **MAX66040** и **MAX66140** — это конечные изделия для вполне конкретных приложений. Основная отличительная особенность новых изделий — наличие встроенных функций криптозащиты SHA-1. Сам по себе алгоритм SHA-1 не лучше и не хуже других, подобных ему. Тот или иной алгоритм применяют различные производители,

поскольку выбор алгоритма криптозащиты на данный момент не регламентирован каким-то глобальным стандартом, а является исторически сложившейся практикой конкретной компании. Применение SHA-1 в приложениях контроля доступа — это своеобразная визитная карточка компании Maxim, отработанная на множестве «таблеток» iButton, например, на изделиях **DS1961S** или **DS1963S**, которые нашли применение не только в системах контроля доступа, но и в различных приложениях eCash (электронные деньги) в качестве носителей информации. С этой точки зрения MAX66x40 являются хорошей функциональной заменой для DS1961S. Поэтому появление RFID-идентификаторов MAX66040 и MAX66140 позволяет с минимальными усилиями перевести хорошо зарекомендовавшие себя СКД-приложения, реализованные на «таблетках», на более современный, более удобный в использовании и просто более эстетичный форм-фактор носителя информации. Именно с этим связан параллельный выпуск двух модификаций: под стандарты ISO/IEC 14443B (proximity card) и ISO/IEC 15693 (vicinity card). Применение «таблеток» требовало непосредственного контакта со считывателем. Причем, поскольку и ключи, и считыватели создавались одной компанией и появились одновременно, то вопрос о различных стандартах просто не возникал. Для RFID-приложений уже сложилось два направления: высокоскоростной обмен данными в непосредственной близости от считывателя, или малая скорость на большем расстоянии. У разных разработчиков могут быть разные условия или предпочтения, поэтому предложены оба варианта функциональной замены.

Заключение

Отметим, что компания Maxim в линейке RFID-продуктов не предлагает чипы. Предлагаются только брелки и бесконтактные карты, то есть законченные изделия-идентификаторы. Как законченные изделия ключи компании Maxim не имеет смысла сравнивать с простейшими бесконтактными ключами множества производителей Юго-Восточной Азии и других регионов. Основное предназначение моделей MAX66040 и MAX66140 — замена контактных «таблеток» с реализованным алгоритмом хеширования SHA-1 на бесконтактные proximity- и vicinity-решения в тех системах контроля доступа, где компоненты Maxim успешно зарекомендовали себя в исполнении iButton.⁵

Получение технической информации,
заказ образцов, поставка —
e-mail: analog.vesti@compel.ru

Александр Калачев (г. Барнаул)

ДЛЯ RFID С ИНТЕЛЛЕКТУАЛЬНОЙ РЕГИСТРАЦИЕЙ: ПАМЯТЬ С ДВОЙНЫМ ИНТЕРФЕЙСОМ ОТ STM



Выпускаемая компанией **STMicroelectronics** **EEPROM M24LRxxx** с параллельным взаимодействием по двум независимым каналам (I²C и радиointерфейс) и значительными объемами хранимых данных идеальна для использования в современных устройствах **радиочастотной идентификации**.



Одной из последних тенденций современности является становление так называемого «Интернета вещей» (Internet of things) — совокупности устройств, способных взаимодействовать друг с другом, выполняя при этом определенные функции. Иногда это кажется излишеством, но во многих случаях небольшие автоматизированные или автоматические устройства способны составить элегантное решение многих прикладных задач — сбор показаний датчиков, фиксация событий, мониторинг состояния объектов, управление приборами и устройствами. Популярность и сфера применения небольших автономных устройств с сетевыми возможностями постоянно растет. Этому немало способствует уменьшение их размеров и стоимости, а также — развитие программной инфраструктуры в виде стеков протоколов и библиотек приложений.

Интересной разновидностью мобильных беспроводных систем является класс устройств, не требующих для своего функционирования собственного источника питания. Их питание осуществляется за счет получения энергии от внешнего электромагнитного поля. Они становятся активными в некоторой области вблизи источника радиоволн определенной частоты. Вероятно когда-нибудь они достигнут возможностей, описанных в романе В. Винджа «Глубина в небе» (создание полноценной сети с возможностью передачи звука и изображения). На данный момент устройства с питанием от радиоимпульсов, так называемые радиочастотные, или RFID-метки, способны передавать в ответ на запрос некоторую идентифицирующую информацию с возможностью записи новых данных.

RFID-устройства

Идентификационные данные и показатели работы, передаваемые RFID-

устройствами в зависимости от объекта автоматизации и решаемых задач могут использоваться как самостоятельно, так и совместно с информационными ресурсами внешних информационных систем.

На территории Российской Федерации разрешены для свободного использования следующие диапазоны рабочих частот:

- НЧ — 125...134 кГц;
- ВЧ — 13,56 МГц;
- УВЧ — 865...868 и 915...921 МГц;
- микроволны — 2,4 ГГц.

Рабочая частота выбирается из диапазонов, разрешенных к свободному использованию частот, с учетом следующих факторов:

- максимального расстояния считывания:
 - для НЧ — несколько сантиметров;
 - для ВЧ — 0,5...0,6 м;
 - для УВЧ — до нескольких метров;
 - для микроволн — до 200...300 метров;
- типа прикладной системы идентификации;
- условий эксплуатации;
- цены устройств.

Основные области применения RFID лежат в системах:

- обеспечения безопасности:
 - идентификация личности;

- ключ допуска в помещение;
- отслеживание перемещений товара или оборудования;
- системы «антивор»;
- сбора данных (т.н. «дatalogгеры»);
- логистики.

Можно также выделить и новые тенденции, такие как смена режима работы мобильных вычислительных устройств в зависимости от окружения. В частности, появляются приложения для устройств на платформе Android с поддержкой NFC (Near Field Communications), позволяющие активировать те или иные приложения в зависимости от расположенной рядом метки. Данную идею вполне можно распространить и на более серьезные задачи, например, запрет или разрешение доступа к данным или приложениям в зависимости от окружения — офис, удаленный офис, конференц-зал, дом.

В нашей стране пока наиболее распространены RFID-системы, использующие диапазоны НЧ и ВЧ (125...134 кГц и 13,56 МГц соответственно), считается, что в системах контроля доступа, отслеживания выноса товара и т.п. они менее чувствительны к попыткам блокировки работы.

Семейство EEPROM с двойным интерфейсом доступа

Обычно RFID-устройства представляют собой электрически стираемую

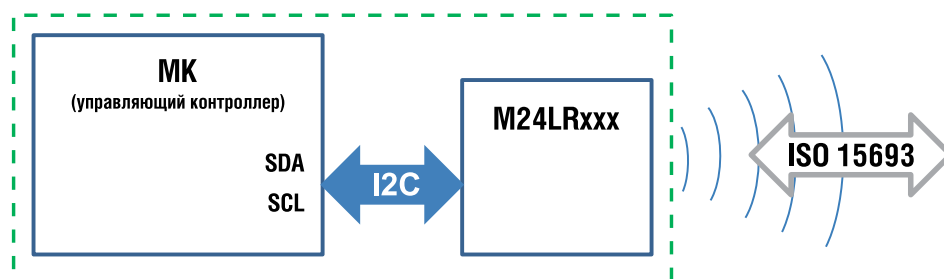


Рис. 1. Типовая структура системы, использующей память с двойным интерфейсом

Таблица 1. Семейство микросхем EEPROM с двойным интерфейсом M24LRxxx

Наименование	Емкость, кбит	Корпус
M24LR04E-R	4096	SO-8; TSSOP8; UDFPN 8 2x3x0,6
M24LR16E-R	16384	SO-8; TSSOP8; UDFPN 8 2x3x0,6
M24LR64-R	65536	SAWN WAFER F 8; SO-8; TSSOP8; UDFPN 8 2x3x0,6
M24LR64E-R	65536	SO-8; TSSOP8; UDFPN 8 2x3x0,6

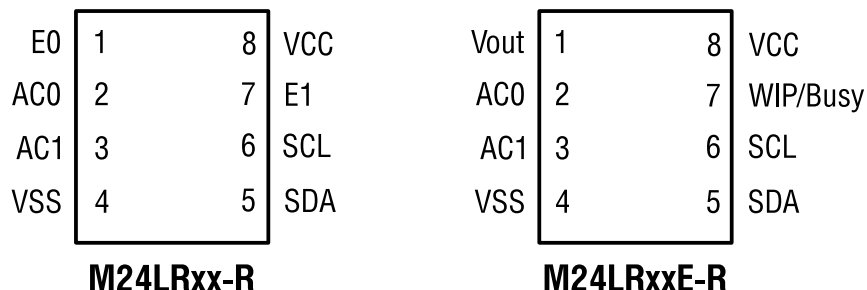


Рис. 2. Отличия в выводах между сериями M24LRxx и M24LRxxE

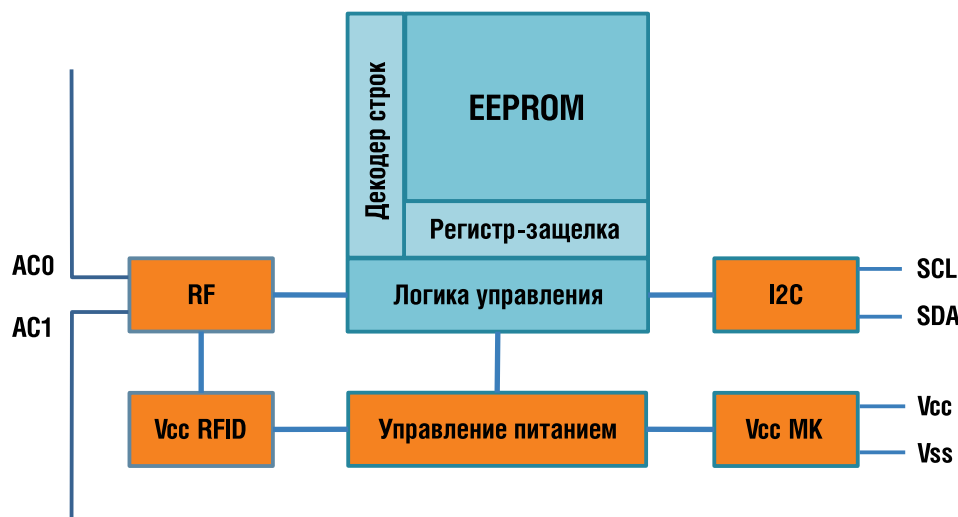


Рис. 3. Структурная схема EEPROM M24LRxxx

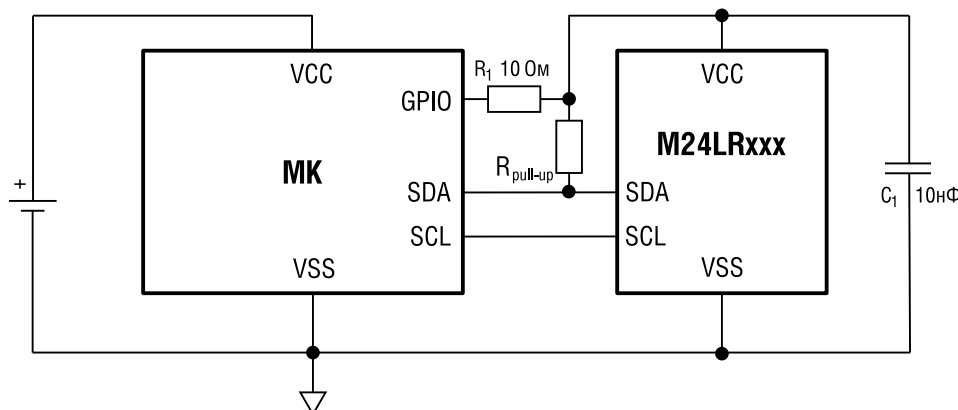


Рис. 4. Типовая схема включения M24LRxxx

энергонезависимую память с доступом по радиоканалу. STMicroelectronics предлагает оригинальное семейство EEPROM **M24LRxxx** с двойным интерфейсом доступа — данные доступны по интерфейсу I²C и по радиointерфейсу стандарта ISO 15693, работающему

на частоте 13,56 МГц [1, 2]. По каждому из интерфейсов данные защищены 32-битным паролем доступа — один пароль для I²C-шины и четыре пароля для доступа по радиоканалу. Данные, записанные в EEPROM по интерфейсу I²C, могут быть прочитаны либо смартфо-

ном со встроенным ISO 15693-совместимым NFC-интерфейсом, либо обычным RFID-считывателем.

Память с двойным интерфейсом, хотя и проигрывает в размерах обычным RFID-устройствам, не имеющим корпуса, но открывает целый спектр новых возможностей (рис. 1), сочетая достоинства внешней энергонезависимой памяти и памяти с бесконтактным доступом.

В семейство M24LRxxx входят микросхемы EEPROM емкостью от 4 до 64 кбит (таблица 1) [1]. Серии **M24LRxxE** имеют выход индикации наличия поля и выход индикации обращения к памяти по радиоканалу, в серии **M24LRxx** вместо данных выводов расположены выводы выбора адреса (рис. 2) [2].

Структурная схема M24LRxxx представлена на рисунке 3.

Основные характеристики:

- диапазон напряжений питания 1,8...5,5 В;
- ток потребления (при питании со стороны I²C-интерфейса):
 - в режиме чтения 50 (V_{cc} = 1,8; f_{scl} = 100 кГц)...400 (V_{cc} = 5,5; f_{scl} = 400 кГц) мкА;
 - в режиме записи 220 мкА;
 - в режиме ожидания 30...40 мкА.
- режимы одиночного чтения и чтения последовательных блоков;
- рабочие тактовые частоты I²C-интерфейса 25...400 кГц;
- со стороны I²C-интерфейса доступ к данным осуществляется побайтно, со стороны радиointерфейса — блоками по 32 бита;
- более 1 миллиона циклов перезаписи;
- время записи — по I²C < 5 мс, по радиоканалу 5,75 мс;
- время хранения данных до 40 лет.

Для разрешения конфликтов одновременного доступа к памяти по I²C и по радиоканалу семейство M24LRxxx имеет встроенную схему арбитража.

В схему арбитража входит:

- менеджер питания, отслеживающий наличие питания от внешнего источника или поля;
- арбитр доступа, отслеживающий режим доступа к памяти со стороны радиоканала и шины I²C.

Основные правила арбитража следующие:

- при отсутствии питания на линии VCC доступ к памяти возможен только по радиоканалу;
- при наличии и поля считывателя, и проводного питания выполняется первая из распознанных команд, пришедшая или по радиоканалу, или по шине I²C, и до завершения ее выполнения остальные команды игнорируются.

Типовая схема включения памяти M24LRxxx представлена на рисунке 4 [3].

Представленная схема включения является одной из оптимальных с точки зрения применения в системах с ограниченными ресурсами энергии (необходимость длительной автономной работы, батарейное питание). Низкий ток потребления позволяет питать EEPROM непосредственно от выходной линии порта микроконтроллера. При необходимости для серий M24LRxxE приложение может использовать выходы индикации наличия поля считывателя и доступа к EEPROM по радиоканалу. В случае применения контроллера с ультранизким энергопотреблением, к примеру, одного из контроллеров STMicroelectronics линейки **STM8L**, общее потребление устройства будет лежать в пределах 1 мкА (потребление STM8L в режиме Active-Alt).

Дополнительно:

- в режиме ожидания также отключается питание M24LRxxx и нет утечки тока через подтягивающий резистор на линии SDA;

- в активном режиме работы контроллера приложение полностью управляет питанием EEPROM, подавая его только при необходимости обращения к памяти по I²C.

Индуктивность антенны, подключаемой к выводам AC0, AC1, рассчитывается таким образом, чтобы резонансная частота параллельного колебательного контура, образованного индуктивностью антенны и встроенной емкостью (параметр Ctuning) была равна 13,65 МГц. В зависимости от требуемого форм-фактора конечного устройства возможно применение печатных петлевых антенн (примеры таких антенн также доступны на сайте STMicroelectronics; кроме того, в ряде старых справочников по радиотехнике приводятся расчетные формулы для печатных индуктивностей различных конфигураций) или SMD-индуктивностей [4].

Серии M24LRxx допускают параллельное подключение для наращивания емкости памяти [4]. Это достигается путем параллельного подключения M24LRxx к одной шине I²C, параллельного подключения к одной антенне и задания разных уровней на линиях выбора адреса (E0, E1). Таким образом, возможно объединение до четырех микросхем M24LRxx, что при использовании, например, микросхем серии **M24LR64-R** позволяет получить объем суммарной памяти до 256 кбит (32 кбайта) — см. рис. 5. В данном включении со стороны считывателя параллельно включенные EEPROM будут видны как несколько отдельных микросхем, и доступ к ним будет осуществляться по их уникальным серийным номерам. Со стороны I²C доступ к отдельным микросхемам осуществляется по различным адресам шины I²C.

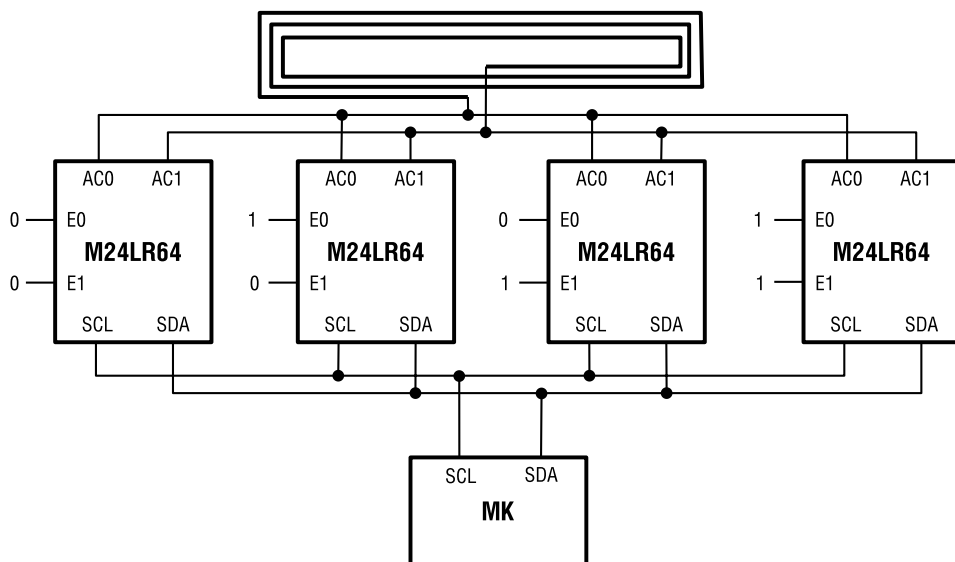


Рис. 5. Объединение M24LR64-R для увеличения суммарного объема памяти

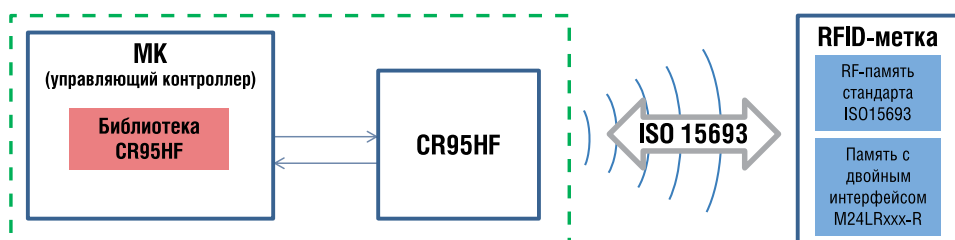


Рис. 6. Типовая структура RFID-считывателя на базе CR95HF

При параллельном подключении EEPROM на одну антенну следует помнить, что их встроенные емкости Ctuning будут суммироваться, и требуемая индуктивность антенны будет меньше в количество раз, равное количеству параллельно включенных микросхем памяти.

Основные области применения EEPROM с двойным интерфейсом:

- промышленная автоматика, системы сбора данных, медицинское оборудование — обеспечение обновления/

актуализации калибровочных данных, обновление параметров конфигураций, считывание диагностических показаний;

- периферийные устройства, телекоммуникационное оборудование, бытовая электроника — обновление параметров конфигураций, считывание диагностических показаний, активация оборудования, запись настроек локализации, отслеживание перемещений;

- RFID-системы — регистраторы данных, идентификационные карточки, регистраторы передвижения/перемещения персонала или объектов.

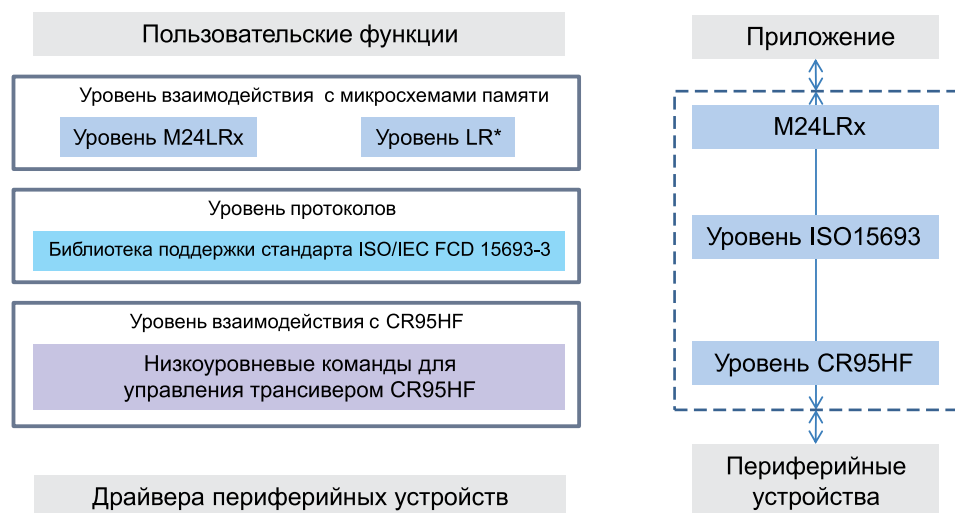


Рис. 7. Структура библиотеки для работы с трансивером CR95HF

Таблица 2. Доступные отладочные наборы и оценочные платы EEPROM с двойным интерфейсом

Наименование	Описание	Микросхема EEPROM, лежащая в основе
Оценочные платы EEPROM с антеннами различных типов, мм		
<u>ANT1-M24LR-A</u>	Плата с M24LR64-R с петлевой печатной антенной, размер 45x75	<u>M24LR64-R</u>
<u>ANT1-M24LR16E</u>	Плата с M24LR64E-R с петлевой печатной антенной, 45x75	<u>M24LR16E-R</u>
<u>ANT2-M24LR-A</u>	Плата с M24LR64-R с петлевой печатной антенной, 20x40	<u>M24LR64-R</u>
<u>ANT2-M24LR16E</u>	Плата с M24LR64E-R с петлевой печатной антенной, 20x40	<u>M24LR16E-R</u>
<u>ANT3-M24LR-A</u>	Демонстрационная плата с M24LR64-R с SMD-индуктивностью в качестве антенны	<u>M24LR64-R</u>
<u>ANT4-M24LR-A</u>	Демонстрационная плата с двумя параллельно включенными M24LR64-R (общая емкость EEPROM 128 кбит)	<u>M24LR64-R</u>
<u>ANT5-M24LR-A</u>	Демонстрационная плата с четырьмя параллельно включенными M24LR64-R (общая емкость EEPROM 256 кбит)	<u>M24LR64-R</u>
<u>ANT7-M24LR16E</u>	Демонстрационная плата с M24LR16E-R с двухслойной печатной антенной 15x15	<u>M24LR16E-R</u>
<u>FLEX-M24LR04E</u>	Демонстрационная плата с M24LR04E-R на гибкой основе с антенной 45x75	<u>M24LR04E-R</u>
<u>ROBOT-M24LR16E-A</u>	Демонстрационная плата с M24LR16E-R, выполненная в виде силуэта робота, с печатной антенной 20x40	<u>M24LR16E-R</u>
Демонстрационные и отладочные платы с приемопередатчиком CR95HF		
<u>DEMO-CR95HF-A</u>	Демонстрационная плата трансивера CR95HF	<u>CR95HF</u>
<u>PLUG-CR95HF-B</u>	Демонстрационная плата трансивера CR95HF	<u>CR95HF</u>
Регистраторы данных		
<u>DATALOG-M24LR-A</u>	Регистратор данных на базе M24LR64-R с управляющим контроллером SMT8L и датчиком температуры STTS75	<u>M24LR64-R</u>
<u>STEVAL-IPR002V1</u>	Регистратор данных на базе M24LR64-R с управляющим контроллером STM8L, датчиками температуры, влажности, вибрации, свободного падения, освещенности	<u>M24LR64-R</u>
Отладочные наборы		
<u>DEMOKIT-M24LR-A</u>	Демонстрационный набор для работы с EEPROM M24LRxx-R (RFID-считыватель, антенна считывателя, I ² C-программатор)	<u>M24LR64-R</u>
<u>DEVKIT-M24LR-A</u>	Отладочный набор для работы с EEPROM M24LRxx-R (RFID-считыватель, антенна считывателя, I ² C-программатор, плата ANT1-M24LR-A)	<u>M24LR64-R</u>
<u>M24LR-DISCOVERY</u>	Отладочный набор для работы с M24LR04E	<u>M24LR04E-R</u>

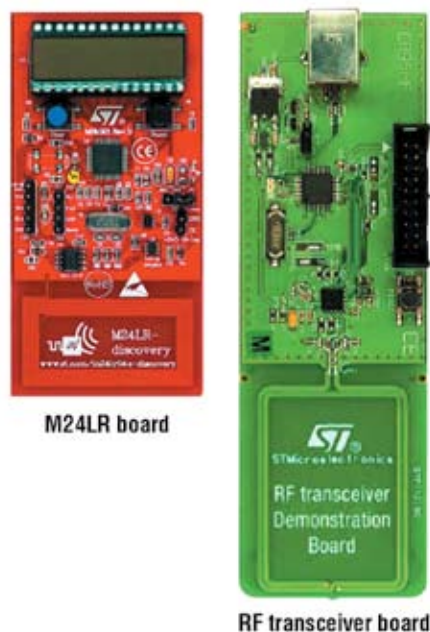


Рис. 8. Отладочный набор M24LR- DISCOVERY

Считыватель RFID-меток CR95HF

Для работы с RFID-устройствами, в частности, с EEPROM с двойным интерфейсом, STMicroelectronics предлагает приемопередатчик **CR95HF** [5, 6]. CR95HF поддерживает стандарты ISO 14443A/B, ISO 15693, а также протокол NFC (ISO/IEC 18092).

Трансивер CR95HF работает в режиме ведомого устройства, управляемого внешним хост-контроллером (рис. 6). Для работы с трансивером доступна библиотека, позволяющая достаточно просто взаимодействовать с ним посредством SPI- или UART-интерфейса.

Библиотека доступна для скачивания с официального сайта STMicroelectronics в вариантах как для 32-разрядных контроллеров **STM32**, так и для бюджетных энергоэффективных 8-битных STM8L [6].

В состав библиотеки входит три уровня (рис. 7):

- нижний уровень — CR95HF LL, содержащий низкоуровневые команды для непосредственного управления трансивером CR95HF;

- средний уровень — уровень протоколов, отвечающий за поддержку и выполнение протокола стандарта ISO/IEC FCD 15693-3;

- верхний уровень — уровень взаимодействия с микросхемами памяти, содержащий команды управления памятью семейств **M24LRxxx** и **L1Rxxx**.

Для пользовательского приложения все три уровня являются прозрачными и представляются только функции самой библиотеки.

Ознакомительные и отладочные платы

STMicroelectronics предлагает широкий выбор отладочных средств и ознакомительных плат для начала работы с EEPROM с двойным интерфейсом [7]. Данные инструменты позволяют разра-

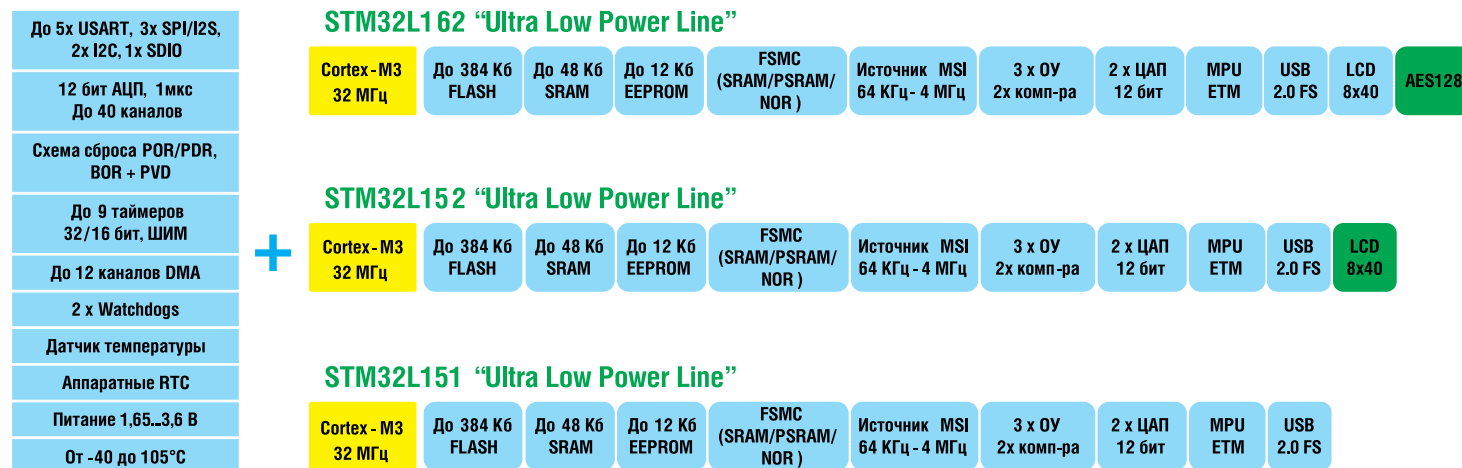


Рис. 9. Семейство STM32L

ботчику оценить расстояния, на которых возможно успешное считывание по радиоканалу, влияние типа антенн считывателя и памяти на условия совместной работы. Отладочные наборы позволяют:

- работать с EEPROM в режиме доступа по шине I²C и в режиме доступа по радиоканалу;
- исследовать работу механизмов разделения памяти на блоки, защиты отдельных блоков, работы механизмов парольной защиты.

Доступные отладочные наборы и оценочные платы EEPROM с двойным интерфейсом представлены в таблице 2.

Одним из наиболее простых, но функциональных отладочных наборов является набор **M24LR-DISCOVERY** [8], включающий в себя две платы (рис. 8): M24LR board с памятью и плату с приемопередатчиком CR95HF:

Плата **M24LR board** содержит микросхему памяти с двойным интерфейсом **M24LR04E-RMN6T/2** (4 кбит, корпус SO8N), контроллер **STM8L152C6T6** с 8 кбайт флеш-памяти, датчик температуры **STTS751-0WB3F**, печатную антенну 20x40 мм, ЖК-индикатор. Имеет разъемы EEPROM (I²C) для программирования и отладки программ контроллера (SWIM).

M24LR board также может работать с телефонами и коммуникаторами на базе Android с поддержкой NFC. Соответствующее приложение NfcV-Reader доступно в репозитории приложений Google Play и позволяет при помощи телефона, просматривать данные, зафиксированные платой.

Плата приемопередатчика (RF transceiver board) включает в себя трансивер **CR95HF-VMD5T** 13,56 МГц, контроллер **STM32F103CB** с 128 кбайт флеш-памяти, печатную антенну 47x34 мм. Интерфейс с хост-компьютером и питание платы осуществляется через USB.

Программные продукты для работы с отладочным набором доступны по адресу www.st.com/m24lr04e-discovery,

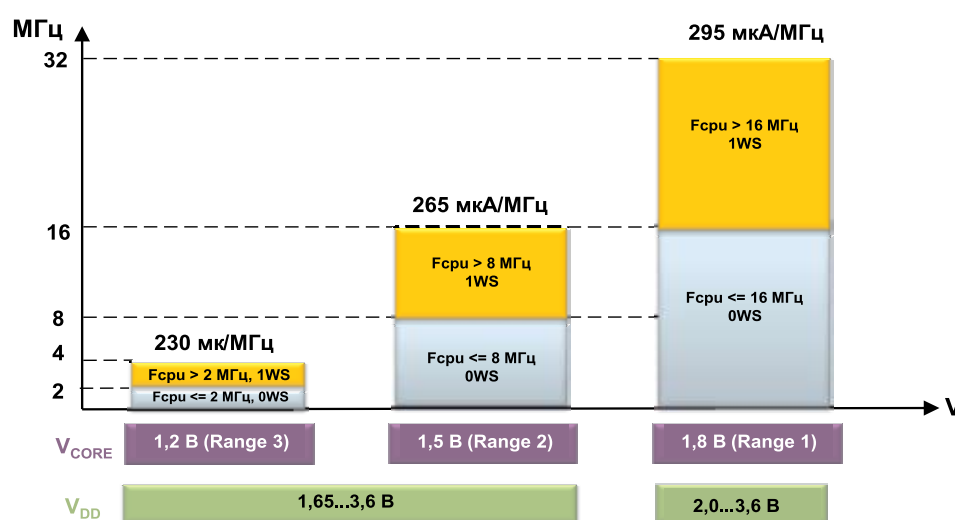


Рис. 10. Зависимость производительности от напряжения питания ядра

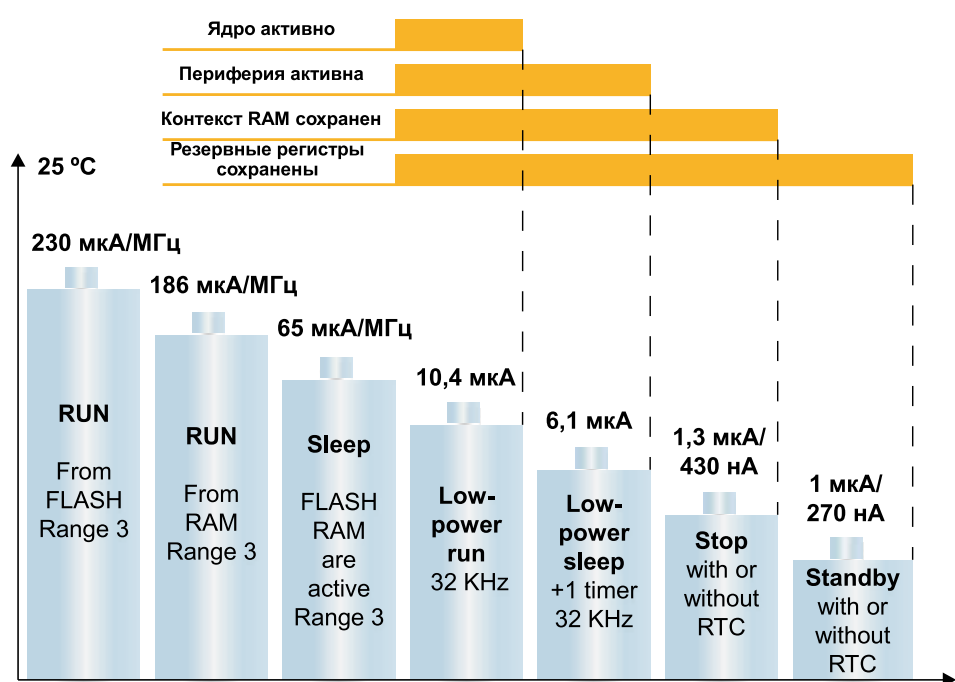


Рис. 11. Режимы энергопотребления STM32L

они включают в себя программу для хост-компьютера и скомпилированный образ приложения для STM8L. Отла-

дочные платы набора также содержат запрограммированные образы демонстрационных приложений.

STM8L162 "Additional Performance Level"

Ядро STM8 16 МГц	До 64 Кб FLASH	До 4 Кб SRAM	До 2 Кб EEPROM	RESET BOR/PVD	Внешний источник 1-16 МГц	RTC	DMA 4 канала	АЦП, 1мкс 12 бит	2 x ЦАП 12 бит	LCD 8x40	AES128
---------------------	-------------------	-----------------	-------------------	------------------	---------------------------------	-----	-----------------	---------------------	-------------------	-------------	--------

STM8L151/152 "Performance Level"

Ядро STM8 16 МГц	До 64 Кб FLASH	До 4 Кб SRAM	До 2 Кб EEPROM	RESET BOR/PVD	Внешний источник 1-16 МГц	RTC	DMA 4 канала	АЦП, 1мкс 12 бит	2 x ЦАП 12 бит	LCD* 8x40
---------------------	-------------------	-----------------	-------------------	------------------	---------------------------------	-----	-----------------	---------------------	-------------------	--------------



STM8L101 "Entry Level"

Cortex-M3 32 МГц	До 8 Кб FLASH	1.5 Кб SRAM	До 2 Кб EEPROM
---------------------	------------------	----------------	-------------------

STM8L05 "Value Line Level"

Ядро STM8 16 МГц	До 64 Кб FLASH	До 2 Кб SRAM	128 байт EEPROM	RESET BOR/PVD	Внешний источник 1-16 МГц	RTC	DMA 4 канала	АЦП, 1мкс 12 бит	LCD 8x40
---------------------	-------------------	-----------------	--------------------	------------------	---------------------------------	-----	-----------------	---------------------	-------------



* - только в STM8L152

Рис. 12. Номенклатура микроконтроллеров STM8L

Микроконтроллеры с низким энергопотреблением от STMicroelectronics

Зачастую для работы с памятью с двойным интерфейсом необходим микроконтроллер, и желательно, чтобы он потреблял как можно меньше энергии. Для таких задач STMicroelectronics предлагает две линейки микроконтроллеров — **STM32L** и **STM8L**.

Линейка STM32L является отличным компромиссом между высоким быстродействием, свойственным архитектуре Cortex-M3, и низким энергопотреблением. Последнее достигнуто за счет специальной технологии производства и оптимизированной периферии. Обзор линейки STM32L приведен на рисунке 9.

Производительность микроконтроллера измеряется в DMIPS/МГц и зависит от функциональной составляющей ядра, интерфейса памяти и периферии. Само же энергопотребление мА/DMIPS в процессе работы может быть макси-

мизировано с помощью регулирования напряжения питания. Именно метод, динамической адаптации напряжения питания в зависимости от необходимой частоты тактирования микроконтроллера был применен в STM32L. При работе МК на максимальной частоте (для полного использования всех его возможностей — производительности, периферии) обычно необходимо, чтобы верхняя граница питающего напряжения составляла 3...3,3 В. Если контроллеру необходимо переключиться в режим низких частот тактирования, это напряжение является избыточным и приводит к лишним затратам энергопотребления. Для устранения этого в линейке STM32L реализовано динамическое изменение напряжения ядра микроконтроллера. STM32L предоставляет возможность динамического изменения напряжения питания ядра в трех диапазонах: 1,8 В (Range 1); 1,5 В (Range 2) и 1,2 В (Range 3) (рис 10).

Такая особенность позволяет добиться общего снижения энергопотребления более чем на 25%. Таким образом, конфигурирование напряжения питания ядра в совокупности с режимами ультранизкого энергопотребления позволяет подходить к регулированию потребления более гибко. Общие режимы энергопотребления микроконтроллеров наглядно продемонстрированы на рисунке 11.

Несмотря на большую популярность семейства **STM32**, компания не оставляет без внимания и младшую линейку **STM8L**, расширяя и дополняя ее номенклатуру. Семейство STM8L состоит из четырех линеек (рис. 12).

Отличительные особенности линейки STM8L — это улучшенная аналоговая периферия: быстрый 12-битный АЦП на 24 канала, 12-битный ЦАП, компараторы. Отметим, что микроконтроллеры данной линейки в отличие от большинства своих конкурентов имеют встроенный DMA-контроллер, что позволяет при грамотном подходе к проектированию программного обеспечения значительно повысить производительность.

Во второй половине 2012 года на рынке появилась линейка микроконтроллеров STM8L "Value Line", основным принципом которой является хорошее соотношение цена/функциональность. Снижение цены достигнуто, прежде всего, благодаря техническим новшествам при производстве, снижению затрат за счет параллелизма тестирования конечной продукции. Сама технология производства осталась без изменений, включая технологию производства кристаллов. Основные ограничения — более узкий температурный диапазон -40...85°C; меньший, чем обычно, объем EEPROM-памяти; нет уникального идентификатора и сервиса

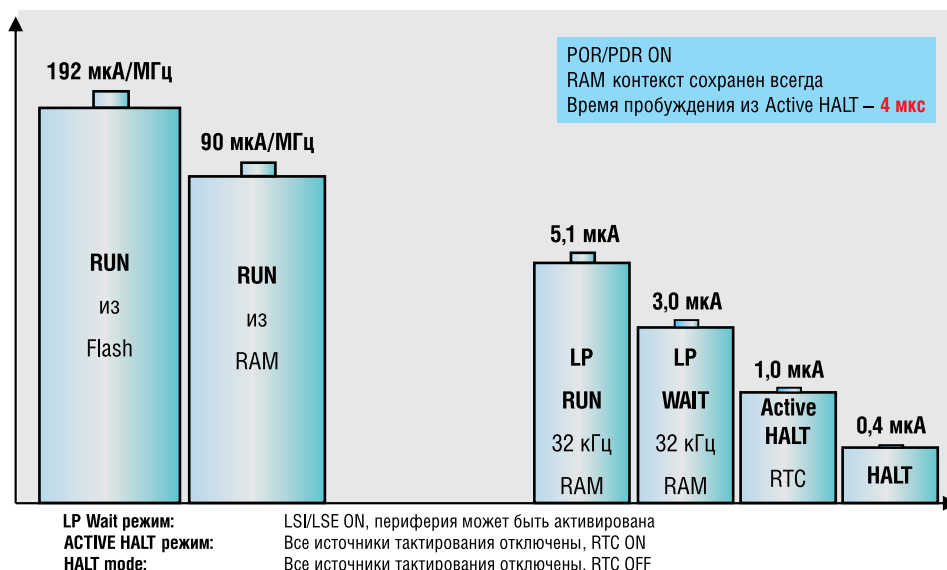


Рис. 13. Режимы снижения энергопотребления микроконтроллеров STM8L

программирования прошивки микроконтроллера на мощностях производителя. Также снижено количество циклов записи/стирания flash- и EEPROM-памяти. Для flash-памяти данный параметр равен 100 во всем температурном диапазоне, для EEPROM это соотношение равно 100 000 циклов.

В остальном микроконтроллеры серии «Value Line» аналогичны по функциональности своим старшим собратьям и также имеют полную выводную (pin-to-pin) и программную совместимость внутри своих линеек. Например, разработчик может легко и без каких-либо изменений использовать в своем проекте STM8L051F3P6 вместо STM8L151F3P6, и наоборот. Ему лишь требуется поменять в свойствах проекта тип микроконтроллера и пересобрать проект заново.

Для низкопотребляющей линейки STM8L, помимо вышеперечисленных ограничений, также снижен набор периферийных модулей — нет компараторов, 12-битного ЦАП, датчика температуры, дизайн портов ввода-вывода не предусматривает подключение сенсорных кнопок.

Для снижения энергопотребления контроллеры имеют несколько специальных режимов работы (рис. 13). Более подробную информацию по всем режимам можно посмотреть в документации на микроконтроллер, отметим лишь, что в самом экономичном режиме «HALT» содержимое оперативной памяти SRAM сохраняется и время восстановления в полностью рабочее состояние составляет порядка нескольких микросекунд.

Заключение

Учитывая возможности EEPROM M24LRxxx по параллельному взаимодействию по двум независимым каналам и значительные для RFID-памяти объемы хранимых данных, можно рассмотреть возможность применения ее в системах безопасности, нацеленных на обеспечение конфиденциальности и целостности информации.

В частности, объем памяти позволяет хранить достаточно большое количество событий (например, доступ в те или иные помещения), что может помочь при расследовании инцидентов. Возможно также использование связки контроллер+CH95HF и M24LRxxx в качестве:

- аппаратных ключей для активации оборудования или приложений на рабочем месте сотрудника, чтобы предотвратить несанкционированный доступ во время его отсутствия;
- хранилища ключей шифрования, исключающего возможность перехвата или копирования информации;
- хранилища контрольных сумм важных документов или системных

файлов для отслеживания нежелательной программной активности или контроля целостности документов.

Наличие интерфейса I²C позволяет создавать интеллектуальные регистраторы событий на основе микроконтроллеров, фиксирующие, в зависимости от периферийных датчиков, различный набор параметров или событий. Кроме того, данная возможность имеет большие перспективы в области отслеживания движения грузов и товара, благодаря возможности фиксации температурного режима, условий перевозки, отслеживания перемещений по складу или территории магазина. Снятие этих данных при приеме товара от перевозчика позволит разрешить ряд вопросов, связанных с выявлением дефектов товара (их появление при производстве, погрузке или транспортировке).

Литература

1. Dual Interface EEPROM//<http://www.st.com/internet/mcu/class/1766.jsp>.
2. Андрей Никитин. Двухпортовая память M24LR64 с интерфейсами I²C и RFID//Новости электроники, 2010, №8, с. 20-22.
3. How to manage simultaneous I²C and RF data transfers with the M24LRxx-R and M24LRxxE-R devices//http://www.st.com/internet/com/TECHNICAL_RESOURCES/TECHNICAL_LITERATURE/APPLICATION_NOTE/CD00247968.pdf.

LITERATURE/APPLICATION_NOTE/CD00247968.pdf.

4. M24LR64-R Multi-bank reference design description and settings//http://www.st.com/internet/com/TECHNICAL_RESOURCES/TECHNICAL_LITERATURE/APPLICATION_NOTE/CD00280653.pdf.

5. CR95HF library for ISO15693 and Dual Interface EEPROM products//http://www.st.com/internet/com/TECHNICAL_RESOURCES/TECHNICAL_LITERATURE/APPLICATION_NOTE/DM00025202.pdf.

6. Using the CR95HF library with STM8L microcontrollers//http://www.st.com/internet/com/TECHNICAL_RESOURCES/TECHNICAL_LITERATURE/APPLICATION_NOTE/DM00039049.pdf.

7. Eval boards for Memory ICs//<http://www.st.com/internet/evalboard/subclass/1444.jsp>.

8. M24LR-DISCOVERY — STMicroelectronics//<http://www.st.com/internet/evalboard/product/253360.jsp>.

Получение технической информации,
заказ образцов, поставка —
e-mail: memory.vesti@compel.ru

EEPROM память с радиоинтерфейсом

M24LRxxx

- От 4 до 64 Кбит EEPROM
- RFID + I²C доступ
- Малое потребление
- Более 1М циклов
- 1,8...5,5 В напряжение питания

Поддержка разработчиков:
E-mail: st@compel.ru
www.compel.ru/projects-support

Компэл
www.compel.ru

Андрей Самоделов (Москва)

ПЕРЕДАЧА ДАННЫХ БЕЗ ПРОБЛЕМ: МОДЕМЫ И ПРИЕМОПЕРЕДАТЧИКИ ОТ ON SEMICONDUCTOR



На первый взгляд, новые приемопередатчики **ON Semiconductor NCN49597/9 (PLC-модем с S-FSK-модуляцией), NCV7471 (LIN/CAN) и NCN5120 (KNX)** не имеют прямого отношения к теме безопасности. Но это — если узко понимать слово «безопасность». А в современном широком понимании надежная и **помехозащищенная передача данных** самым непосредственным образом связана с этой тематикой. Да и системы безопасности как таковые невозможно построить без интерфейсов.



Общая безопасность систем передачи данных зависит от многих факторов, к которым относятся физическая надежность приемопередающих устройств и возможность их резервирования/вывода из сети в случае поломки; надежность канала передачи данных; помехозащищенность на уровне используемых типов модуляции/демодуляции сигнала и ряд других факторов.

В данной статье будет рассмотрено несколько новейших микросхем компании ON Semiconductor (таблица 1), предназначенных для использования в различных сетях передачи данных.

Описание используемых стандартов передачи данных

S-FSK-модуляция. Сетка частот CENELEC A-D

S-FSK-модуляция (spread frequency shift keying, частотная манипуляция с расширением спектра) определена стандартом IEC 61334-5-1 и является усовершенствованным вариантом частотной манипуляции (FSK). При FSK-модуляции значения 0 и 1 передаются определенными частотами (как правило, синусоидального) сигнала с постоянной амплитудой. Частотная манипуляция обеспечивает большую помехозащищенность, чем амплитудная модуляция, поскольку сигнал помехи оказывает наибольшее воздействие на амплитуду сигнала, а не на его частоту.

Основное отличие между FSK и S-FSK заключается в том, что при S-FSK-модуляции разное частот, кодирующих 0 и 1 (F0 и F1) информационной последовательности, существенно больше, чем при модуляции FSK, и составляет 10 кГц, причем это значение не зависит от скорости передачи данных. Большой разнос частот позволяет уве-

личить помехоустойчивость при наличии узкополосных помех и сохранить простоту реализации метода.

В стандарте IEC 61334-5-1 не регламентируются значения частот F0 и F1, которые выбираются в соответствии с рекомендациями CENELEC в зависимости от используемой полосы частот. Кроме того, в стандарте IEC 61334-5-1 приведены спецификации физического (PHY) уровня и канального подуровня MAC (*Media Access Control*) для PLC-систем с S-FSK-модуляцией.

Сетка частот CENELEC, принятая Европейским комитетом по электротехнической стандартизации (*European Committee for Electrotechnical Standardization*), регулирует низкочастотную передачу данных в диапазоне 0...500 кГц и разбита на четыре полосы (A-D), которые описаны в таблице 2.

Для сеток Cenelec A, B, D уровень протокола определяется стандартами или патентами. Для сетки Cenelec C определен доступ по стандарту CSMA (*Carrier Sense Multiple Access*, Множественный доступ с контролем несущей).

Шина CAN

Шина CAN (*Controller Area Network*) была предложена Робертом Бошем (*Robert Bosch*) в 80-х годах для автомобильной промышленности, затем стандартизована ISO (ISO 11898) и SAE (*Society of Automotive Engineers*). В настоящее время большинство европейских автомобильных концернов (например, Audi, BMW, Renault, Saab, Volvo, Volkswagen) используют ее в системах безопасности, обеспечения комфорта и управления движением. В Европе вводится единый интерфейс для систем компьютерной диагностики автомобиля, который разрабатывается на базе шины CAN. В ближайшее время в каждом автомобиле европейского производства будет хотя бы один узел, поддерживающий этот интерфейс.

CAN представляет собой асинхронную последовательную шину, использующую в качестве среды передачи обычную витую пару проводов. При скорости передачи 1 Мбит/с длина шины может достигать 30 м. Максимальная длина шины, в соответствии со стандартом, составляет 1 км. При необходимости обмениваться информацией

Таблица 1. Список рассмотренных микросхем

Тип микросхемы	Назначение	Стандарт обмена данными
NCN49597	PLC-модем	S-FSK модуляция
NCN49599	PLC-модем с Phy-интерфейсом	Сетка частот CENELEC A-D
NCV7471	LIN/CAN-приемопередатчик	LIN, CAN
NCN5120	KNX-приемопередатчик для витой пары	KNX

Таблица 2. Сетка частот Cenelec

Сетка	Диапазон частот, кГц	Назначение
Cenelec A	0...95	Исключительно для поставщиков электроэнергии
Cenelec B	95...125	Открыты для использования любыми приложениями
Cenelec C	125...140	
Cenelec D	140...148	

Таблица 3. Характеристики шины CAN

Параметр	Значение
Топология	Последовательная шина, с обоих концов линии стоят заглушки с сопротивлением 120 Ом
Среда передачи данных	Витая пара с волновым сопротивлением 120 Ом
Обнаружение ошибок	15-битный CRC-код
Локализация ошибок	Различают ситуации с постоянной и временной ошибкой. Устройства с постоянной ошибкой отключаются от шины
Текущая версия	CAN 2.0B
Скорость передачи, Мбит/с	До 1
Длина шины, м	До 30 (при максимальной скорости передачи)
Количество устройств на шине	64 (теоретически не ограничено)

на больших расстояниях используются мосты и повторители. Теоретически число подсоединяемых к шине устройств не ограничено, практически — до 64. Это обусловлено нагрузочной способностью стандартных приемопередатчиков. Шина не имеет выделенного мастера, поэтому управлять ею могут сразу несколько устройств. Основные характеристики шины CAN приведены в таблице 3.

Существует две версии шины CAN:

1. Версия А задает 11-битную идентификацию сообщений (максимум 2048 функций).

2. Версия В задает 29-битную идентификацию сообщений (максимум 536 млн. функций).

Версия В, часто именуемая FullCAN, все больше вытесняет версию А, которую называют также BasicCAN.

Сеть CAN состоит из узлов с собственными тактовыми генераторами. Любой узел сети CAN посылает сообщение сразу всем системам, подсоединенным к шине, которые при получении сообщения решают, относится ли оно к данному блоку. Для этого в CAN-контроллерах имеется аппаратная фильтрация сообщений. Таким образом одна посланная команда может привести в действие для своего выполнения произвольное количество подсистем. Если исполнителей команды много, то такой способ передачи и обработки команд обеспечит значительный выигрыш по сравнению с адресным способом.

Каждый подключенный к CAN-шине блок имеет определенное входное сопротивление, в результате образуется общая нагрузка шины CAN. Общее сопротивление нагрузки зависит от числа подключенных к шине электронных блоков управления и исполнительных механизмов. Следует учитывать, что при выключении питания происходит отключение нагрузочных резисторов модулей, подключенных к CAN-шине.

Основные неисправности CAN-шины связаны с замыканием/обрывом линий (или замыканием нагрузочных резисто-

ров на них), снижением уровня сигналов на шине, нарушениями в логике ее работы. В последнем случае поиск дефекта может обеспечить только анализатор CAN-шины.

В мире производится множество типов CAN-контроллеров, которые имеют общую структуру:

- Обработчик протокола (CAN protocol handler)
- Фильтр сообщений
- Память для сообщений
- Интерфейс с ЦП.

Во многих современных микроконтроллерах имеется встроенный контроллер шины CAN.

Шина CAN продолжает развиваться в нескольких направлениях. В новом проекте стандарта предполагается увеличить скорость передачи данных, так как в автомобиле появилось много компьютерных подсистем, связанных с передачей аудио- и видеoinформации. Необходимость повышения надежности требует введения дублированной шины CAN.

Шина LIN

Для низкоскоростной электроники до недавнего времени никаких стандартов не было, и каждый производитель был вынужден придумывать свои собственные системы. Для решения задач обмена данными в таких системах был утвержден стандарт LIN.

Технические требования протокола LIN (*Local Interconnection Network*) разработаны и утверждены Европейским автомобильным консорциумом как дешевое дополнение к сверхнадежному протоколу CAN. Протокол LIN предназначен для низкоскоростного (до 20 кбит/с) обмена данными на коротких расстояниях. Он служит для передачи входных воздействий, состояний переключателей на панелях управления и так далее, а также ответных действий различных устройств, соединенных в одну систему через LIN, происходящих в так называемом «человеческом» временном диапазоне (порядка сотен миллисекунд). Основные задачи, возлагаемые на стандарт LIN консорциумом

европейских автомобильных производителей — объединение автомобильных подсистем и узлов (таких как дверные замки, стеклоочистители, стеклоподъемники, управление магнитолой и климат-контролем и так далее) в единую электронную систему.

Стандарт LIN включает технические требования на протокол и на среду передачи данных. Как последовательный протокол связи, LIN эффективно поддерживает управление электронными узлами в автомобильных системах с шиной класса «А» (двухнаправленный полудуплексный), что подразумевает наличие в системе одного главного (master) и нескольких подчиненных (slave) узлов.

Особенности LIN

Протокол LIN поддерживает двухнаправленную передачу данных по одному проводу длиной до 40 м, используя недорогой микроконтроллер с генератором на RC-цепочке, без кварцевого резонатора. Идеология стандарта — как можно больше задач переложить на программное обеспечение с целью уменьшения стоимости конструкции. При каждом сеансе обмена данными контроллеры автоматически проводят самосинхронизацию. В основу LIN положена концепция «single-master/multi-slave», обеспечивающая дешевое исполнение, основанное на стандартных последовательных периферийных модулях UART/SCI.

Шину LIN можно перевести в режим микропотребления (Sleep mode), когда она выключается (переходит в состояние с высоким импедансом). Любой узел на шине, при необходимости, может включить ее вновь. Протокол LIN отличается от шины CAN низкой стоимостью за счет пониженной эффективности. Структура шины представляет собой нечто среднее между I²C и RS-232. Шина подтягивается к источнику питания через резистор, установленный в каждом узле, и вниз через открытый коллекторный переход приемопередатчика, как в I²C. Вместо линии тактирования каждый передаваемый байт обрамляется стартовым и стоповым битами и передается асинхронно, как в протоколе RS-232.

Диапазон изменений напряжения питания лежит в пределах 9...18 В, но все узлы должны выдерживать перегрузки и сохранять работоспособность при увеличении напряжения на шине вплоть до 40 В. Микроконтроллер (который может иметь обычное напряжение питания 3,3 или 5 В) в каждом узле подключается к шине через приемопередатчик, который и обеспечивает необходимую защиту от перегрузок.

Протокол LIN, ввиду своей простоты и невысокой скорости обмена данными

ми, допускает как программную, так и аппаратную реализацию.

Стандарт KNX

Стандарт KNX появился путем соединения нескольких европейских шинных систем. Среди них Европейская установочная шина EIB (*European Installation Bus*), которая с 1992 года начала успешно завоевывать рынок. Популярность стандарта EIB привела к тому, что на его базе в мае 1999 года произошло слияние трех европейских систем (EIB, BatiBus, EHS) в один стандарт KNX. Владелец уже мирового стандарта KNX является международная ассоциация Konnex Association (в прошлом EIBA). Помимо разработки стандартов и норм, ассоциация занимается контролем качества и совместимости продукции от разных производителей, согласованием рекламной и торговой политики фирм-производителей, имеющих право на использование торгового знака KNX/EIB.

Стандарт KNX поддерживается десятками ведущих европейских производителей электротехнической продукции, что обеспечивает возможность работы в одной KNX-системе устройств различных производителей.

Шина KNX является единственным общемировым открытым стандартом в области автоматизации управления от квартиры до группы зданий. Кроме того, KNX является лидирующим стандартом автоматизации зданий и широко

используется во всем мире для конструирования «умных домов» и «интеллектуальных зданий».

Установочная шина KNX/EIB представляет собой распределенную систему, для которой не требуется шинный контроллер (master). Все устройства на шине соединяются в сеть одним сигнальным кабелем типа «витая пара». Прокладывается и подключается сразу два кабеля: по одной паре проводов передается сигнал; вторая пара — резервная.

Как правило, шинная система KNX/EIB включает в себя следующие элементы:

- KNX-датчики, которые измеряют и подают сигнал о состоянии, например выключатели, панели управления, термостаты, датчики протечки или датчики открытия окон/дверей;
- KNX-актуаторы, или «исполнители», которые выполняют команды, например актуаторы жалюзи, светорегуляторы, клапаны перекрытия воды, актуаторы-выключатели;
- системные устройства, такие как блоки питания, соединители линий, различные модули логики, IP-маршрутизаторы, GSM-шлюзы;
- KNX-шина, «сигнальная линия», которая обеспечивает питанием слаботочные компоненты системы и одновременно служит физической средой для передачи данных.

Для обмена информацией в системе KNX используются четыре среды пере-

дачи данных: передача данных через шину; передача данных по электросети с помощью PLC-модемов; передача данных по радиоканалу (частота 868 МГц); передача данных по сети Ethernet.

Для примера использования KNX-технологии рассмотрим различия между традиционной электропроводкой и KNX-электропроводкой.

Различия между традиционной проводкой и электропроводкой по KNX-технологии

В традиционной электропроводке (220 В) потребители включаются/выключаются с помощью обычных выключателей, для чего требуется прокладка силового кабеля (220 В) к каждому выключателю и потребителю.

В KNX-системе силовая электропроводка (220 В) прокладывается только между исполнительными устройствами шины (актуаторами) и потребителями, а все датчики (выключатели, термостаты и др.) с актуаторами соединяются низковольтной (30 В) слаботочной KNX-шиной. Благодаря этому силовая часть выполняется без обходных путей, что уменьшает расход силового кабеля, количество соединений, потерь, избавляет от необходимости прокладки дополнительных каналов для силового кабеля и, как следствие, снижает вероятность возникновения короткого замыкания, пожара.

При традиционной электропроводке для каждого потребителя или группы

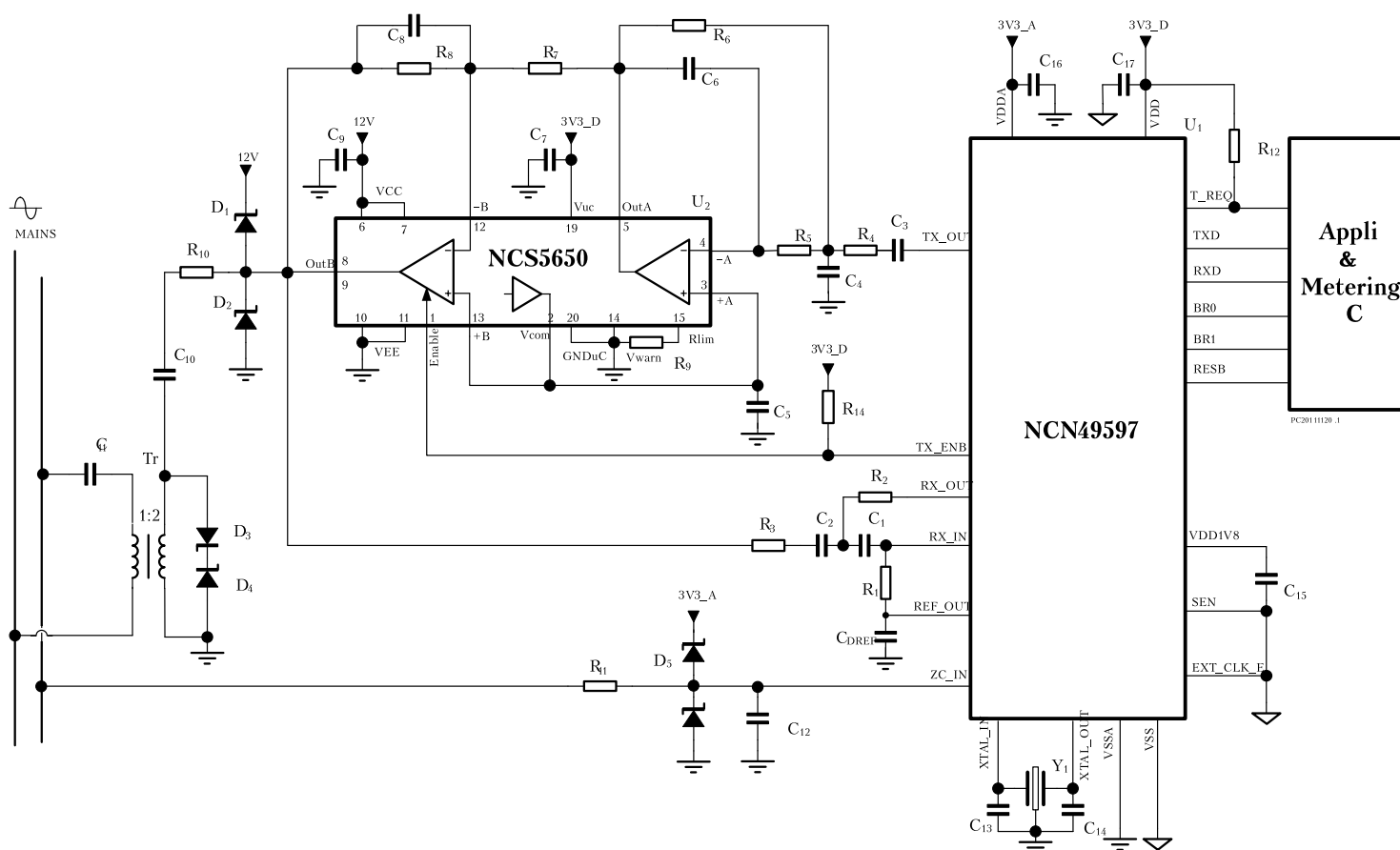


Рис. 1. Схема включения PLC-модема NCN49597

Таблица 4. Основные параметры PLC-модемов NCN49597/49599

Параметр	Значение
Назначение	Полудуплексный PLC-модем
Частота питающей сети, Гц	50 и 60
Модуляция	Два канала с S-FSK-модуляцией
Максимальная скорость обмена, бод	4800 на канал; 9600 в режиме двух каналов
Встроенный процессор	Cortex M0
Тип ПО	Программируемое встроенное ПО
Сертификация	IEC 61334-5-1 и CENELEC EN 50065-1
Программируемый диапазон частот	CENELEC A-D
Программируемая скорость обмена (частота сети)	300, 600, 1200, 2400, 4800 бод (50 Гц); 360, 720, 1440, 2880, 5760 бод (60 Гц)
Обеспечение надежности обмена	Повтор сообщений и алгоритм интеллектуальной синхронизации
Интерфейс ко внешнему микроконтроллеру	SCI: UART/Full Duplex UART
Защита от сбоев	Функция аварийной сигнализации
Скорость обмена по SCI-интерфейсу, кбод	9,6; 19,2; 38,4; 115,2
Напряжение питания, В	3,3
Рабочий температурный диапазон, °C	-40...125

Таблица 5. Основные функциональные особенности NCV7471

Управляющая логика	Обеспечивает безопасную последовательность включения и корректирует реакцию на различные условия электропитания Управляет режимом обмена данными, включая управление электропитанием и обработку сигналов вывода из режима пониженного энергопотребления, локального пробуждения (через вывод WU) и циклического пробуждения (с использованием встроенного таймера) Генерирует сигнал сброса и запросы на прерывания
Последовательный периферийный интерфейс (SPI)	Работает с 16-битными фреймами Обеспечивает обмен данными с микроконтроллерным блоком ECU Через восемь 12-битных регистров осуществляется выбор режимов работы, снятие информации о состоянии микросхемы и работа со сторожевым таймером (watchdog)
Напряжение питания 5 В V_{OUT} от DC/DC-преобразователя	Может обеспечить выходной ток до 500 мА при стабильности 2% Может использоваться для питания микроконтроллера ECU Пригодно для старт-стоповых систем с напряжением батареи питания не менее 2,5 В
5 В V_{OUT2} выходной стабилизатор с низким падением напряжения	Может обеспечивать питание внешних устройств, например, датчиков Управляется через SPI-интерфейс и машину состояний Защищен от короткого замыкания аккумулятора автомобиля
Высокоскоростной CAN-приемопередатчик	Соответствует ISO11898 Защищает от доминантного таймаута по линии TxD
Два LIN-приемопередатчика	Соответствуют LIN2.1 и J2602 Защищают от доминантного таймаута по линии TxD
Вход пробуждения WU	Чувствительный к перепаду уровня высоковольтный вход Может использоваться как источник сигнала пробуждения микросхемы или как логический вход, опрашиваемый через SPI
Функции защиты и мониторинга	Мониторинг силовой линии в точке V_{MID} Мониторинг выхода источника питания VOUT с программируемым порогом Диагностика источника питания VOUT2 через SPI-интерфейс и прерывание Предупреждение о перегреве и температурная защита Программируемый сторожевой таймер (watchdog) для мониторинга ПО ECU

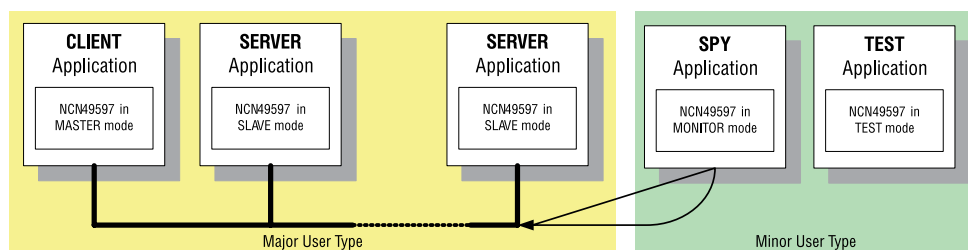


Рис. 2. Пример использования PLC-модемов NCN49597/49599

потребителей прокладывают отдельный кабель, а для каждой прикладной системы управления (охранной, противопожарной, системы доступа) — отдельную кабельную сеть, что уже сейчас воспринимается как архаизм. Широкий ассортимент разработанных устройств позволяет автоматизировать все системы жизнеобеспечения в здании и на прилегающей территории (освещение, отопление, охрана, вентиляция, поливка газо-

нов и др.) и объединить их в единую управляемую сеть инфраструктуры.

Помимо экономии проводов, KNX-системы обладают и другими преимуществами:

- **На порядок упрощается электроустановка в здании.**

При этом значительно сокращаются затраты на ее проектирование и прокладку, поскольку у силовых кабельных сетей остается лишь одна задача — подвод электропитания к потребляющим устройствам.

- **Беспроблемное расширение или изменение системы.**

В случае изменения назначения помещений устройства шины просто переставляются или перепрограммируются без прокладки новых проводов.

- **Простое и удобное управление устройствами**

Способствует созданию комфортных условий в доме и приводит к существенной экономии средств при рациональном расходе энергоресурсов.

Управлять KNX-системами можно как локально (в отдельном помещении), так и централизованно (с диспетчерского пульта или компьютера). Кроме того, несложно организовать удаленное управление с мобильного телефона с помощью SMS или через сеть Интернет.

Перейдем к рассмотрению продукции **ON Semiconductor**.

PLC-модемы NCN49597/NCN49599

Микросхемы **NCN49597/49599** — это PLC-модемы, удовлетворяющие спецификации IEC 61334-5-1 и использующие S-FSK-модуляцию для надежного обмена данными на низких скоростях по силовым линиям. Обе микросхемы построены на базе процессора с ядром ARM Cortex M0 и включают MAC-уровень. NCN49599 содержит, кроме этого, приемопередатчик физического уровня, что позволяет строить на ней однокристалльные PLC-модемы. Для изготовления NCN49597 используется технология смешанных сигналов ON Semiconductor, позволяющая объединять цифровые и аналоговые схемы на одном кристалле ИС.

На рисунке 1 приведена схема включения PLC-модема NCN49597, а в таблице 4 — его основные параметры.

PLC-модемы NCN49597/49599 находят широкое применение в автоматизированных системах удаленного считывания информации с датчиков, удаленном управлении охранными системами и уличным освещением.

На рисунке 2 показан пример использования PLC-модемов NCN49597/49599

NCN49597/49599 предназначены для подключения оборудования с использованием DLC-сетей (Distribution

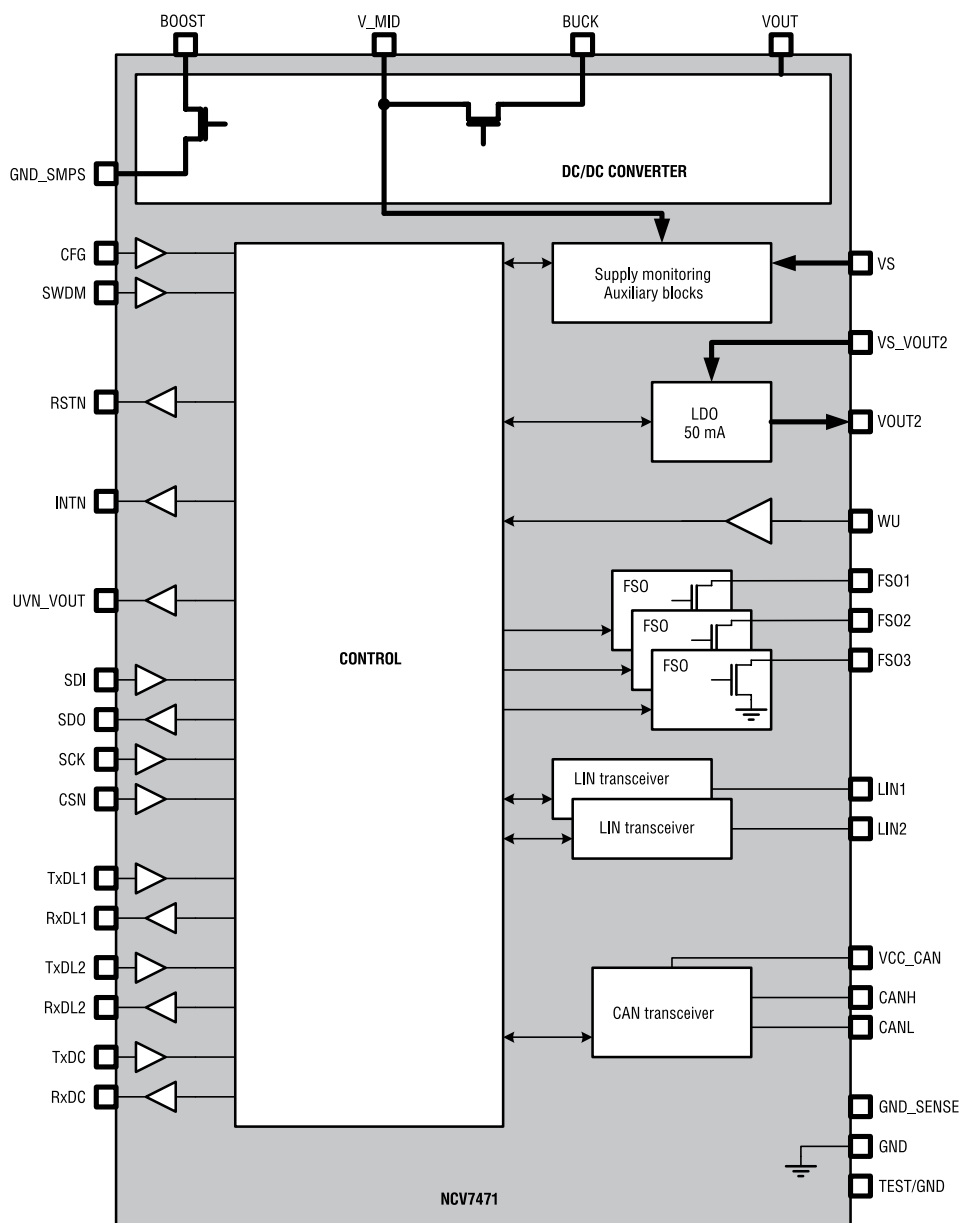


Рис. 3. Блок-схема NCV7471

Line Carrier). Они могут обслуживать два главных и два вспомогательных типа приложений.

Главные типы приложений:

- Мастер (ведущий) или Клиент:

Мастер является клиентом в системе сбора данных от одного или нескольких ведомых, подключенных к силовой линии. Он собирает данные от ведомых устройств и управляет ими. Типичным примером приложения является концентратор систем сбора данных.

- Ведомый или Сервер:

Ведомый представляет данные Мастеру. Типичным примером использования является счетчик электроэнергии с PLC-модемом.

Вспомогательные типы приложений:

- Системы наблюдения или мониторинга:

Системы наблюдения или мониторинга используются только для наблюдения за данными, которые циркулируют

по силовым сетям. В них проверяется корректность только физического уровня фреймов. Если фрейм безошибочный, то данные передаются на обработку внешнему процессору.

- Режим тестирования:

Режим программного тестирования используется для проверки соответствия PLC-модема спецификации CENELEC EN 50065-1 путем непрерывного широкополосного вещания f_s или f_m .

NCV7471: базовый системный кристалл

NCV7471 — это базовый системный кристалл (System Basis Chip, SBC), объединяющий функции, типичные для автомобильных электронных блоков управления (Electronic Control Units, ECUs). На NCV7471 реализуются управляемые низковольтные источники питания для микроконтроллерных приложений и других типов нагрузок.

Таблица 6. Выбор интерфейса обмена данными для NCN5120

TREQ	MODE2	MODE1	SCK/UC2	CSB/UC1	SDI/RXD	SDO/TXD	Описание режима работы
0	0	0	0	0	RXD	TXD	9-бит UART, 19200 Бод
0	0	0	0	1			9-бит UART, 38400 Бод
0	0	0	1	0			8-бит UART, 19200 Бод
0	0	0	1	1			8-бит UART, 38400 Бод
1	0	0	X	X	Драйвер	Приемник	Аналоговый режим
TREQ	0	1	SCK (выход)	CSB (выход)	SDI	SDO	SPI Master, 125 кБод
TREQ	1	0					SPI Master, 500 кБод

Таблица 7. Микросхемы ON Semiconductor для систем обмена данными

Применение	Тип обмена данными							Защита
	PLC		Беспроводной	Проводной				Защита по току
	Узкополосный PLC-модем	KNX PLC-модем	ZigBee	Mbus (проводной)	KNX TP	CAN	HART/Profibus	Устройства защитного отключения (УЗО)
	AMIS30585 AMIS49587 NCN49597 NCN49599 NCN49598	NCN49597 NCN49599	NCS36510	NCN5150 NCN5151	NCN5120	AMIS42670 AMIS42671 AMIS42673 AMIS42675 AMIS42770	A5191HRTLГ A5191HRTPG A5191HRTN NCN5192 AMIS49200 AMIS49250	NCS37000 NCS37005 NCS37010 NCS37012 NCS38000
Интеллектуальные измерительные системы	+	—	+	+	+	—	—	—
Автоматизация зданий	+	+	+	—	+	—	—	—
Интеллектуальные системы освещения	+	+	+	—	—	—	—	—
PV-панели	+	+	+	—	+	—	—	+
Уличное освещение	+	+	—	—	—	—	—	—
Зарядные устройства для электромобилей	+	—	—	—	—	+	—	+
Системы управления процессами	—	—	+	—	—	+	+	—
Крупногабаритная бытовая техника	—	+	+	—	—	—	—	+
Системы электрической безопасности	—	—	—	—	—	—	+	—
Промышленные установки	—	—	—	—	—	+	—	—

ки, системы мониторинга прикладного ПО посредством сторожевого таймера (watchdog). Микросхема имеет встроенные высокоскоростные CAN- и LIN-приемопередатчики, которые позволяют ЕСУ управлять множеством коммуникационных точек или работать в качестве маршрутизатора. Встроенный контроллер состояния обеспечивает безопасную последовательность включения микросхемы и поддерживает работу в режимах пониженного энергопотребления с конфигурируемым набором функций, включая пробуждение от сигналов на линиях обмена данными или локального цифрового сигнала WU. Состоя-

ние ряда внутренних блоков NCV7471 можно прочитать посредством микроконтроллера через SPI-интерфейс или использовать для генерации запросов на внешние прерывания. На рисунке 3 приведена блок-схема, а в таблице 5 — основные функциональные особенности NCV7471.

Основное применение NCV7471 находит в системах управления шасси автомобиля

NCN5120: KNX-приемопередатчик для сетей на основе витой пары

NCN5120 — это первая ИС в семействе KNX-приемопередатчиков

от ON Semiconductor, поддерживающая протоколы приема и передачи по KNX-шине. Микросхема представляет собой KNX-сертифицированный EIB-приемопередатчик, имеющий встроенные PHY- и MAC-уровни (TP1-256). Скорость обмена по шине KNX составляет 9600 бод. При обмене данными, интерфейс (UART/SPI) к хост-контроллеру и скорость обмена выбирается программным способом.

На рисунке 4 приведена блок-схема NCN5120.

Выбор интерфейса и скорости обмена данными осуществляется согласно таблице 6.

Система тактирования позволяет работать от недорогого кварца 16 МГц, являющегося промышленным стандартом. Микросхема имеет возможность генерации тактовой частоты 8/16 МГц для внешнего MCU.

Специальный супервизор позволяет отслеживать напряжения на шине KNX. При передаче осуществляется буферизация передаваемых фреймов данных. С целью повышения надежности обмена данными возможно включение функции конфигурируемого количества повторов и опционального автоответчика. Кроме того, возможна работа в аналоговом режиме. В состав NCN5120 входит конфигурируемый входной разветвитель, позволяющий организовать до двух виртуальных узлов, и токовые петли.

Микросхема имеет встроенный линейный стабилизатор 20 В и два высокоэффективных DC/DC-преобразователя с нагрузочной способностью до 100 мА каждый, снабженные системой управления и мониторинга. Эти преобразователи вырабатывают фиксированное напряжение 3,3 В и регулируемое напряжение 3,3...21 В. В NCN5120 имеется режим пониженного энергопотребления (Sleep Mode).

NCN5120 идеально подходит для силовых приложений. Микросхема может использоваться для уменьшения количества элементов конструкции, поддерживая безопасное и надежное подключение к шине благодаря своим особенностям, таким как выбираемый наклон характеристики системы защиты по току, мониторинг напряжения на шине и температуры.

Рабочий температурный диапазон составляет -25...85°C

К основным преимуществам NCN5120 по сравнению с подобными микросхемами других производителей можно отнести высокий уровень интеграции и низкую стоимость внешних компонентов, возможность подключения мощных устройств к KNX-шине и питания от нее, наличие уникальных возможностей при создании улучшенных KNX-систем и гибкость при интеграции в имеющуюся инфраструктуру.

К основным приложениям можно отнести системы домашней автоматизации, а также системы автоматизации зданий и сооружений. Микросхема NCN5120 может использоваться в различных конечных продуктах, таких как интеллектуальные светильники и переключатели, вентиляторы и кондиционеры, термостаты, детекторы дыма и системы пожарной сигнализации.

Преимущества решений ON Semiconductor

Компания ON Semiconductor является мировым лидером по повышению энергоэффективности и постав-

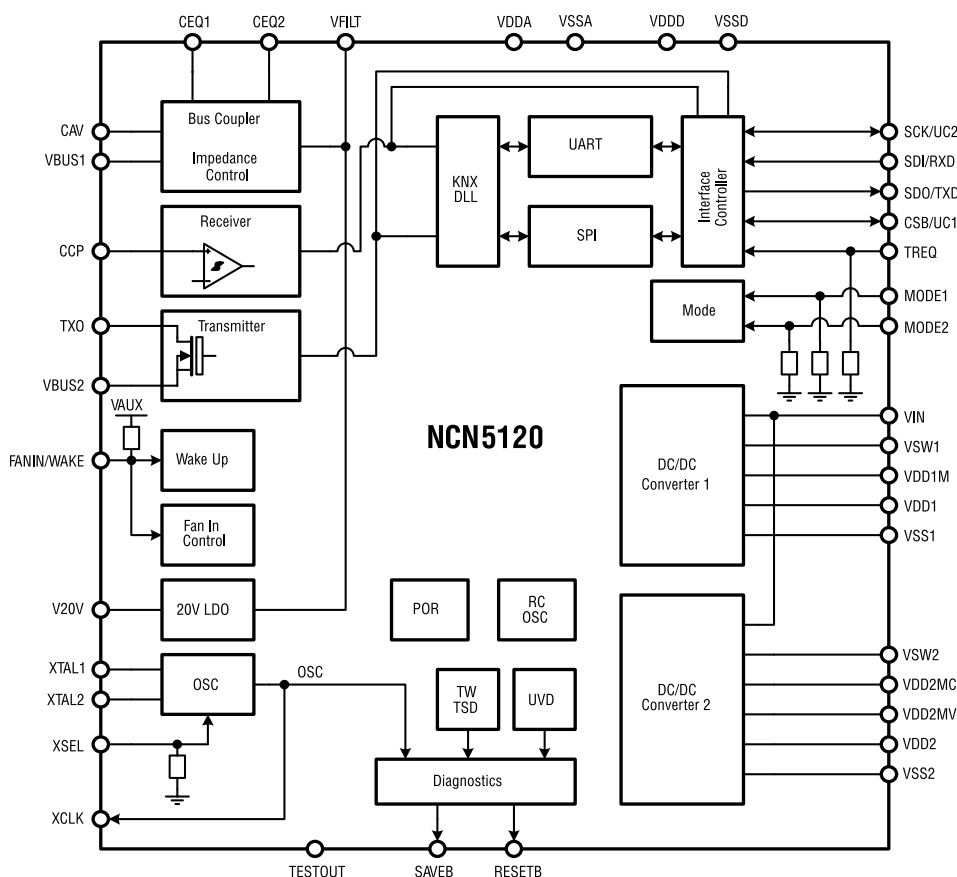


Рис. 4. Блок-схема NCN5120

ляет решения, которые производят, распределяют, потребляют, преобразуют энергию, а также осуществляют мониторинг и управление. На рынок поставлено уже более 5 миллионов PLC-модемов для интеллектуальных энергетических систем. Продукция компании отвечает ведущим мировым стандартам, таким как IEC61334-5-1. Номенклатура микросхем для систем обмена данными и защиты силовых линий покрывает практически все сегменты рынка приложений для интеллектуальных систем сбора и обработки данных, основные из которых приведены в таблице 7. Особое внимание уделяется повышению надежности и безопасности решений.

Литература

1. <http://www.onsemi.com/PowerSolutions/product.do?id=NCN49597>
2. <http://www.onsemi.ru.com/PowerSolutions/product.do?id=NCV7471>
3. <http://www.onsemi.ru.com/PowerSolutions/product.do?id=NCN5120>
4. NCN5120 DC-DC Converter Efficiency Calculator. http://www.onsemi.ru.com/pub/Collateral/NCN5120_CALC.XLSM
5. NCN5120 — KNX Certification Procedure. <http://www.onsemi.ru.com/pub/Collateral/AND9102-D.PDF>

6. KNX Reference Design Evaluation Board User's Manual. <http://www.onsemi.ru.com/pub/Collateral/EVBUM2169-D.PDF>

7. <http://www.onsemi.ru.com/PowerSolutions/product.do?id=NCV7430>

8. Using the Fading Feature of the NCV7430. <http://www.onsemi.ru.com/pub/Collateral/AND9103-D.PDF>

9. Описание стандарта CAN. <http://www.can-cia.de>

10. Андрей Самоделов. Сюиты для счетчика и сети: PLC-решения от ON Semi и STMicro//Новости Электроники №7/2011

11. Андрей Самоделов. Концерт для счетчика и сети: PLC-модемы компании Texas Instruments//Новости Электроники №7/2011

12. Андрей Самоделов. На замену AMIS: новый универсальный PLC-модем компании ON Semiconductor//Новости Электроники №3/2012.

Получение технической информации, заказ образцов, поставка — e-mail: analog.vesti@compel.ru

Свати Джоши (Maxim Integrated)

ЗАЩИТА ОСОБО ВАЖНЫХ ДАННЫХ ПРИ ПОМОЩИ АППАРАТНОЙ РЕАЛИЗАЦИИ МЕХАНИЗМОВ AES

Криптографический блок контроллера MAX36025 DeepCover™, препятствующий несанкционированному извлечению данных, позволяет осуществить эффективную физическую защиту от взлома, тем самым помогая разработчикам обеспечить безопасность в системах нынешнего и последующих поколений. В контроллере применен симметричный алгоритм блочного шифрования Advanced Encryption Standard. Статья представляет собой перевод [1].



Требования безопасности ко всем категориям конечного оборудования стремительно растут. Эта тенденция, в сочетании с риском заражения программными вирусами, приводит к росту значения аппаратной реализации безопасности. Таким образом, разработчики сталкиваются со множеством проблем обеспечения безопасности в системах нынешнего и последующих поколений, в том числе, с вопросом надежного шифрования данных и защиты ключей шифрования.

Для того, чтобы обеспечение безопасности было эффективным, должна быть реализована защита от физического вмешательства, потому что даже самые сложные безопасные микропроцессоры, программируемые вентильные матрицы (FPGA), смарт-карты и другие безопасные компоненты по-прежнему уязвимы для определенных сценариев атаки. Это требует поддержания некоторых цепей в активном состоянии в нерабочий период системы для выявления потенциальных атак, целью которых является извлечение важной информации. Чтобы достичь этого, устройства, обеспечивающие безопасность, должны обладать пониженным уровнем энергопотребления и интерфейсом для работы с несколькими датчиками, задача которых состоит в обнаружении угроз. Также необходимо создать барьеры безопасности вокруг схемы, содержащей чувствительные элементы. Кроме того, когда компонент безопасности может защитить ключи шифрования, а также надежно закодировать данные, это способствует обеспечению более высокого уровня защиты системы и устранению некоторых проблем, с которыми в настоящее время сталкиваются разработчики.

Контроллер с криптографическим блоком, препятствующим несанкционированному извлечению данных,

MAX36025 DeepCover™, выполняет именно эту задачу. Он хранит ключи шифрования в запатентованной* памяти емкостью 1 кбайт без возможности несанкционированного считывания, защищает ключи, осуществляя мониторинг физического вмешательства, а также зашифровывает и расшифровывает данные в двух аппаратных Advanced Encryption Standard (AES)-блоках. Используя атрибуты суще-

ствующих блоков управления безопасностью Maxim, которые обеспечивают надежное хранение в памяти важной информации, MAX36025 также имеет шлюз аутентификации, который осуществляет первичную проверку подлинности любого процессора, пытающегося обратиться к нему, посылая сигнал «запрос-ответ». Процесс аутентификации осуществляется через шифрованный интерфейс I²C, при этом микропроцессор и устройство предварительно снабжены двумя известными ключами. Ключи загружаются в защищенную ячейку памяти MAX36025.

* Патент № 7379325.

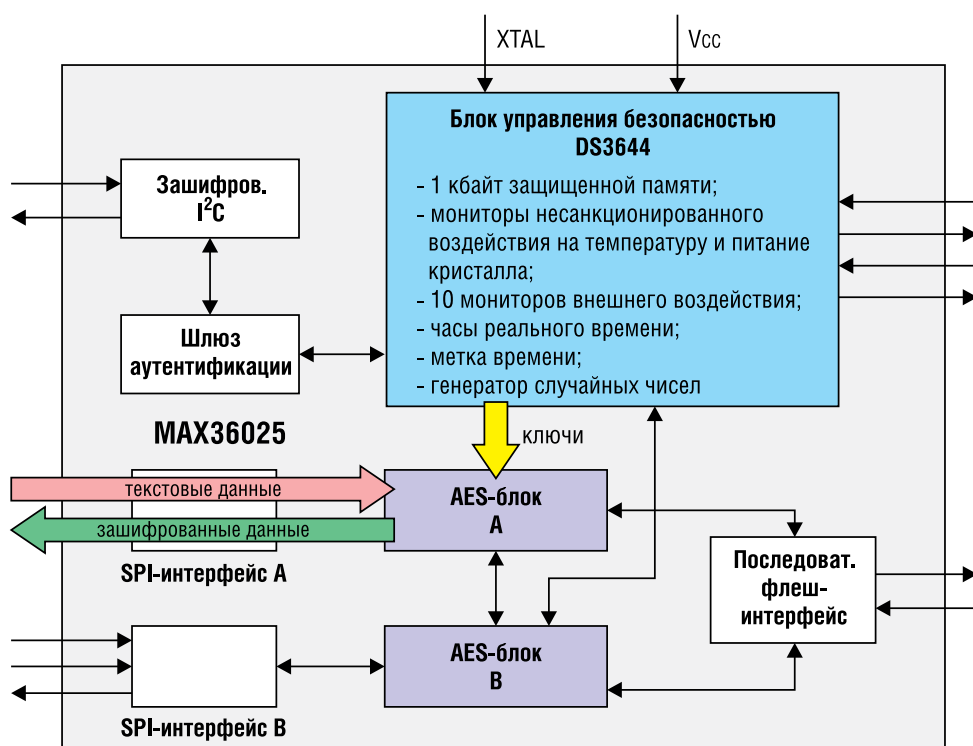


Рис. 1. Использование одного AES-блока для шифрования данных

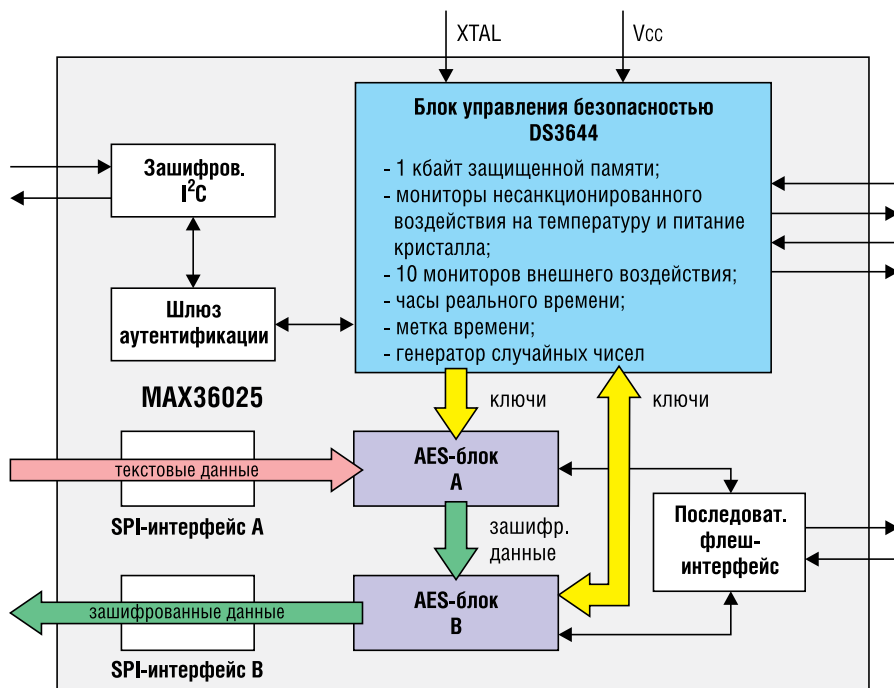


Рис. 2. Использование обоих AES-блоков для шифрования данных

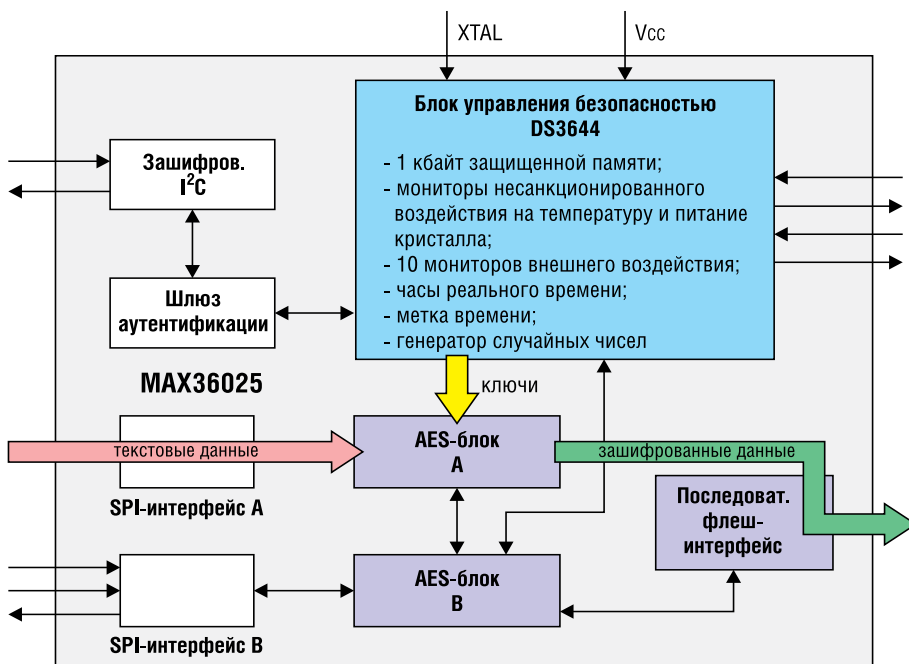


Рис. 3. Хранение зашифрованных данных во внешней последовательной флэш-памяти

Если проверка подлинности не состоится, устройство не позволит получить доступ к внутренней защищенной памяти. После успешной аутентификации ключи шифрования могут быть загружены в защищенную память без возможности несанкционированного считывания. Кроме того, предоставляется доступ к настройке параметров защиты, а также — к маршрутизации данных через два блока AES.

AES-блоки могут работать по разным сценариям (см. рисунки 1...3): зашифровывая и расшифровывая важные данные, или осуществляя обе эти операции с пропускной скоростью 9 Мбит/с. Доступ к AES-блокам возможен через два отдельных двунаправленных SPI-интерфейса. Кроме того, возможна передача большого количества зашифрованных данных через последовательный интерфейс во внешнюю последовательную флэш-память. Это позволяет пользователям безопасно хранить данные в стандартной последовательной флэш-памяти.

MAX36025 — это недавно выпущенный контроллер безопасности, обеспечивающий упрощенный способ реализации AES-шифрования в системе. Будучи стационарным аппаратным устройством, MAX36025 не требует дополнительного кода* для обеспечения обмена с ним данными, тем самым уменьшая время разработки. Эта микросхема является уникальной среди имеющихся на рынке, так как сочетает в себе аппаратные AES-блоки с набором средств обеспечения безопасности, включающим запатентованную память без возможности несанкционированного считывания.

Литература

1. Application Note 5524, Maxim Integrated (<http://www.maximintegrated.com/app-notes/index.mvp/id/5524>).

Получение технической информации,
заказ образцов, поставка —
e-mail: mcu.vesti@compel.ru

ИНЖЕНЕРЫ!

Возможность работать
в дружной команде профессионалов,
внедрять новые электронные компоненты,
изучать передовое, предлагать перспективное!



Контакты: www.compel.ru/jobs
Отдел персонала: +7(495) 234-7757, доб. 2181
Ксения Лисова
E-mail: lisova@compel.ru

Компэл
www.compel.ru

* Небольшое количество кода необходимо для завершения процесса аутентификации.

Гузелия Сафиуллина, Михаил Селезнев (КОМПЭЛ)

«МЫ С КМОП НА ГРАНИЦЕ»: ДАТЧИКИ ИЗОБРАЖЕНИЯ ON SEMICONDUCTOR И ИХ ПРИМЕНЕНИЕ В СИСТЕМАХ БЕЗОПАСНОСТИ

КМОП-датчики изображения, которые в настоящее время выпускаются компанией ON Semiconductor, успешно применяются в системах биометрической идентификации — одном из самых прогрессивных направлений систем обеспечения безопасности. Наиболее перспективным в таких приложениях является датчик изображения IBIS4-6000.



ON Semiconductor®

В январе 2011 года компания **ON Semiconductor** приобрела подразделение CMOS Image Sensor Business Unit компании **Cypress Semiconductor**. Таким образом, номенклатура изделий ONS дополнилась линейкой КМОП-датчиков изображения (CMOS Image Sensor), то есть направлением, в котором компания Cypress работала на протяжении почти 15 лет, являясь одной из первых компаний, которые предложили на рынок КМОП-датчики изображения в качестве не опытных образцов, а серийно выпускаемых изделий.

В настоящее время на рынке представлены датчики, выполненные по одной из двух технологий (если не рассматривать опытные разработки). Это датчики на основе ПЗС-технологии (Приборы с зарядовой связью) и датчики на базе фотодиодных ячеек, выполненных по технологии КМОП. В течение длительного времени КМОП-датчики изображения значительно уступали ПЗС-матрицам по большинству основных параметров и по этой причине не рассматривались как массовая продукция. В конце 90-х годов в производстве КМОП-датчиков были внедрены существенные инновации и в характеристиках изделий ПЗС и КМОП установилось определенное равенство. В линейке изделий Cypress Semiconductor датчики, выполненные по ПЗС-технологии, отсутствовали — компания сконцентрировала усилия на КМОП-технологии, которая и тогда, и в настоящее время представляется более перспективной. Соответственно, и в номенклатуре ON Semiconductor в настоящее время присутствуют только КМОП-датчики.

Рассмотрим основные преимущества датчиков изображения на основе КМОП-матриц по сравнению с ПЗС-матрицами:

1. КМОП-матрицы имеют существенно более низкое энергопотребление в статическом состоянии, что дает возможность применять их в мобильных устройствах с батарейным питанием.

2. Фотоэлементы, схемы обвязки и вычислительные мощности выполнены по одной технологии, что позволяет объединить на одном кристалле оптоэлектронные, аналоговые и цифровые (в том числе микропроцессорные) блоки. Это, в свою очередь, позволяет создать законченную однокристалльную систему с минимальным количеством внешних элементов обвязки, что приводит к уменьшению габаритных размеров конечного устройства, снижению его стоимости и повышению надежности.

3. КМОП-технология обеспечивает возможность прямого доступа к произвольной ячейке матрицы. Соответственно, появляется возможность считывать не весь массив изображения, а либо считать определенный фрагмент, либо «проредить» исходное изображение. Механизм «фрагментированного считывания» позволяет уменьшить объем считываемых данных и, как следствие, повысить частоту кадров видеоустройства. Помимо этого, фрагментирование позволяет с минимальными вычислительными затратами реализовать задачу автоматического расчета экспозиции. В ПЗС-матрицах возможность фрагментирования отсутствовала, поскольку принцип работы предполагал обязательное считывание всего массива данных.

4. Стоимость КМОП-матриц значительно ниже по сравнению с ПЗС-матрицами, причем разница становится особенно заметной при увеличении числа элементов матрицы.

Линейка КМОП-датчиков изображения компании ON Semiconductor

Семейство датчиков VITA включает в себя четыре типа устройств с раз-

мером изображения 1,3...25 мегапикселей. Все четыре типа выпускаются как в монохромном, так и в цветном варианте исполнения. Младшие модели семейства (**VITA1300** и **VITA2000**) могут иметь в качестве канала вывода данных либо высокоскоростной многоканальный LVDS-интерфейс, либо параллельный CMOS-интерфейс. Старшие модели (**VITA5000** и **VITA25K**) имеют только LVDS-интерфейс, поскольку значительный объем информации с матриц не может быть выведен через относительно медленный CMOS-интерфейс за разумное время. Датчики семейства VITA могут работать как в кадровом режиме, так и в режиме скользящего электронного затвора. Отличительной особенностью семейства является реализация мультиоконного режима фрагментирования. Производитель обозначает следующие основные области применения датчиков семейства VITA: промышленные системы технического зрения, **системы мониторинга движущихся объектов, цифровые телекамеры для систем безопасности** (используются как внутри, так и вне помещений, поскольку датчики выпускаются в диапазоне рабочих температур -40...85°C), считыватели двумерных штриховых кодов. Отметим, что наличие кадрового затвора и реализация мультиоконного фрагментирования значительно упрощает реализацию задач слежения за перемещением движущихся объектов на фоне неподвижного ландшафта. В этом смысле датчик VITA-25K, позволяющий отслеживать одновременно до 25 фрагментов при частоте 50 кадров в секунду, безусловно, является уникальным изделием не только для компании ON Semiconductor, но и для отрасли в целом. Характеристики КМОП-датчиков изображения семейства VITA представлены в таблице 1.

Датчики изображения LUPA-300, LUPA-1300-2 и LUPA-3000 предназна-

Таблица 1. Основные параметры КМОП-датчиков изображения компании On Semiconductor

Параметр		VITA-1300	VITA-2000	VITA-5000	VITA-25K	LUPA-300
Размер изображения, пиксел (H*V)		1280*1024	1920*1200	2592*2048	5120*5120	640*480
Размер пиксела, мкм (H*V)		4,8*4,8	4,8*4,8	4,8*4,8	4,5*4,5	9,9*9,9
Оптический формат		1/2 inch	2/3 inch	1 inch	35 мм	1/2 inch
Выходы	LVDS	4 канала	4 канала	8 каналов	32 канала	—
	CMOS	10 бит	10 бит	—	—	10 бит
	Analog	—	—	—	—	—
«Частота кадров, кадров/с»	LVDS	150	90	75	53	—
	CMOS	37	22	—	—	250
Чувствительность, В/лк*сек	@550 нм	4,58	4,58	4,58	3,3	3,2
FPN		0,5	0,5	0,5	0,5	0,1
Динамический диапазон, Дб	Global Shutter	53,2	53,2	53,2	53,2	60,2
	Rolling Shutter	59,8	59,8	59,8	56,6	
Вариант исполнения	Цветной	+	+	+	+	+
	Монохроматический	+	+	+	+	+
Тип затвора	Global Pipelined Master	+	+	+	+	+
	Global Pipelined Slave	+	+	+	+	+
	Global Triggered Master	+	+	+	+	+
	Global Triggered Slave	+	+	+	+	+
	Rolling	+	+	+	+	+
	Normal	+	+	+	+	+
Фрагментирование	ROI	8 окон	8 окон	8 окон	32 окна	1 окно
	Sub-sampled	+	+	+	+	+
Основная частота, МГц		62	62	62	310	80
Разрешение АЦП, бит		8 или 10	8 или 10	8 или 10	8 или 10	10
Рассеив. Мощность, Вт		0,475	0,520	1,000	3,400	0,190
Корпус		LCC-48	LCC-52	LCC-68	μPGA-355	LCC-48

чаются, главным образом, для построения цифровых камер высокоскоростной (с частотой порядка несколько сотен кадров в секунду) видеосъемки. Подобные камеры востребованы в системах автоматизации научных исследований, в оборудовании для проведения экспериментов, в системах контроля и безопасности на некоторых типах промышленных производств. Кроме того, высокоскоростная видеосъемка находит применение в спортивном телевидении (и как элемент спортивных трансляций, и как инструмент для разрешения спорных вопросов при судействе спортивных соревнований). Датчик LUPA-300 имеет скромный по современным меркам размер изображения 640*480 элементов, но может оказаться оптимальным решением для тех приложений, где большой размер изображения не требуется, а востребованы простота реализации и невысокая стоимость. Основными отличительными чертами датчика LUPA-1300-2 являются высокая чувствительность, позволяющая работать на коротких выдержках даже в условиях недостаточной освещенности, а также поддержка мультиоконого фрагментирования. Представляет определенный интерес возможность считывания данных как в прямом, так и в обратном направлении по горизонтали и вертикали, что позволяет реализовать зеркальное отражение картинки аппаратным способом на этапе считывания. Датчик LUPA-3000 является одним из немногих

изделий в отрасли, позволяющим формировать видеозапись с размером кадра 2,9 мегапикселей с кадровой частотой более 400 Гц. Основные области применения датчиков семейства LUPA, помимо высокоскоростной видеосъемки — **телекамеры для систем мониторинга дорожного движения, телевизионные системы для обеспечения безопасности производственных процессов**, системы технического зрения для робототехнических комплексов, медицинская аппаратура. Несколько обособленно стоит 4-мегапиксельный датчик **LUPA-4000**. В отличие от остальных изделий ON Semiconductor, он не содержит аналого-цифрового преобразователя и осуществляет вывод изображения в аналоговой форме по одному или двум каналам. Характеристики датчиков LUPA также приведены в таблице 1. Отметим, что расширенные функциональные возможности датчиков изображения семейств VITA и LUPA в значительной мере превосходят требования стандартных цифровых камер, применяемых в традиционных системах видеонаблюдения и мобильных электронных приборах. Датчики VITA и LUPA ориентированы на применение в высокотехнологичных приложениях, где использование стандартных ПЗС- и КМОП-матриц не обеспечивает решение поставленных задач.

Датчики STAR-250 и STAR-1000 изначально предназначались для задач цифровой астрономии, применения в

космической аппаратуре и других подобных приложениях. Отличительные черты датчиков STAR: повышенная стойкость к радиационному излучению и высокая (по сравнению с матрицами других семейств) повторяемость характеристик фотоэлементов, образующих датчик изображения. Для астрономических задач нет необходимости в применении кадрового затвора (скользящий вполне приемлем, поскольку и камера, и объект съемки неподвижны), не требуется высокая кадровая частота (поэтому вывод осуществляется посредством менее скоростного CMOS-интерфейса), нет особой необходимости в большом размере изображения. На первое по важности место выходит прецизионность характеристик матрицы, что, в целом, и обеспечивают датчики STAR. Параметры датчиков STAR приведены в таблице 1.

В отличие от датчиков изображения семейств VITA, LUPA и STAR, рассмотренных выше, датчики **IBIS4-6600** (наименование для заказа — **NOI4SM6600A-QDC**) и **MANO-9600** по своим функциональным возможностям можно отнести к категории универсальных. То есть, при их проектировании изначально не закладывались функции, необходимые для сравнительно узких, специализированных направлений цифровой фото- и видеосъемки. Функциональные возможности IBIS4 и MANO соответствуют требованиям са-

LUPA-1300-2	LUPA-3000	LUPA-4000	STAR-250	STAR-1000	HAS-2	IBIS4-6600	MANO-9600
1280*1024	1696*1710	2048*2048	512*512	1024*1024	1024*1024	2210*3002	3840*2500
14,0*14,0	8,0*8,0	12,0*12,0	25,0*25,0	15,0*15,0	18,0*18,0	3,5*3,5	2,4*2,4
1 inch	1 inch	35 мм	1 inch	1 inch	35 мм	1 inch	2/3 inch
12 каналов	32 канала	—	—	—	—	—	4 канала
—	—	—	10 бит	10 бит	10 бит	10 бит	10 бит
—	—	66 MSps	—	—	—	—	—
500	485	15	—	—	—	—	20
—	—	—	29	11	4	5	20
10,2	3,8	2,8	5,4	2,7	9,6	2,0	0,5
0,3	0,1	1,45	0,1	0,1	0,1	0,2	0,5
58,0	60,2	—	—	—	—	—	—
+	+	66,0	60,2	н.д.	н.д.	59,0	н.д.
+	+	+	—	—	—	—	—
+	+	+	+	+	+	+	+
+	+	+	—	—	—	—	—
+	+	—	—	—	—	—	—
+	+	—	—	—	—	—	—
+	+	—	—	—	—	—	—
+	+	—	+	+	+	+	+
+	+	+	+	+	+	+	+
4 окна	1 окно	1 окно	1 окно	1 окно	40 окон	1 окно	1 окно
+	+	+	+	+	+	+	+
315	206	33	8	12	5	40	62
10	8 или 10	-	10	10	12	10	8 или 10
1,350	1,100	0,150	0,350	0,400	0,122	0,190	0,510
μPGA-168	μPGA-369	PGA-127	JLCC-84	JLCC-84	JLCC-84	LCC-68	LCC-52

мого широкого спектра практических приложений. Производитель определяет следующие основные области применения этих датчиков: **системы биометрической идентификации**, сканеры общего назначения, системы технического зрения. Характеристики этих устройств оптимальны для монохромной съемки неподвижных или малоподвижных объектов с высоким разрешением в достаточно широком диапазоне освещенности объекта съемки. Основные параметры IBIS4-6600 и MANO-9600 также приведены в таблице 1. Ниже будут отдельно рассмотрены возможности применения датчика IBIS4-6600 в системах биометрической идентификации.

Замечания о некоторых параметрах КМОП-датчиков изображения

Содержание и объем данной статьи не предполагает разъяснения физического смысла даже основных параметров, описывающих фотоэлектрические характеристики ПЗС- или КМОП-датчиков изображения. Это неоднократно было сделано в ряде публикаций. Одно из лучших «введений в тему» предложено в [1].

Следующие параметры, которые, как правило, приводятся в материалах производителя, можно считать за исходные:

1. **Заряд насыщения** (*Saturation Charge или Full Well Charge*) — максимальное количество фотонов, которое

способен захватить один фотоэлемент матрицы. Параметр соответствует «самому светлomu» пикселю.

2. **Темновой шум** (*Dark Noise или Temporal Noise*). Какое-то количество фотонов будет присутствовать в ячейке даже при отсутствии экспонирования. Причины этого явления в данном случае несущественны, важно, что это количество определяет уровень «самого темного» пикселя.

3. **Соотношение «Напряжение на зарядном конденсаторе / Число фотонов»** (*Conversion Gain*). Размерность мкВ/е. Производное от него «Цифровой код / Число фотонов». Выбирается обычно таким образом, чтобы значению заряда насыщения соответствовал максимальный возможный код (или очень близкий к нему).

4. **Чувствительность** (*Sensitivity*). Обычно приводится в размерности «вольт/люкс*секунда». Физический смысл: при освещенности в 1 люкс за 1 секунду на зарядном конденсаторе фотоэлемента возникнет потенциал равный N вольт. Пересчитав вольты в число фотонов, можно определить, за какое время экспонирования при освещенности в 1 люкс фотоэлемент насытится до максимального значения. При прочих равных условиях для больших значений чувствительности это время короче, а для меньших — длиннее. Отметим, что для света с разной длиной волны чувствительность будет различной.

Следующие параметры являются производными от перечисленных выше:

1. **Динамический диапазон**. Определяется на основе таких показателей, как заряд насыщения и темновой шум. Например, для изделия **IBIS4-6600** самому «темному» пикселю соответствует среднеквадратическое значение темнового шума, равное 24 е. Значение заряда полного насыщения равно 21500 е. Отношение второго к первому даст диапазон в 895 раз. Поскольку динамический диапазон измеряется в децибелах, пересчитаем: $20 \cdot \lg(21500/24) = 59,0$ дБ.

Заметим: для 10-ти разрядного АЦП: $20 \cdot \lg(1024/1) = 60,2$ дБ. Значения динамического диапазона в 70, 80 и более децибел в диапазоне возможны только как отношение заряда насыщения к темновому шуму. После 10-разрядного аналого-цифрового преобразования динамический диапазон неизбежно «обрежется» до значения 60,2 дБ.

2. **Шум фиксированного распределения** (*fixed pattern noise — FPN*). Обычно измеряется путем считывания информации с датчика изображения при отсутствии освещения. После этого результат усредняется и выражается в процентах от максимума или в единицах младшего разряда. Если отбросить несущественные детали, то это тот же темновой шум, но применительно не к отдельной ячейке, а по матрице в целом, как интегральная величина.

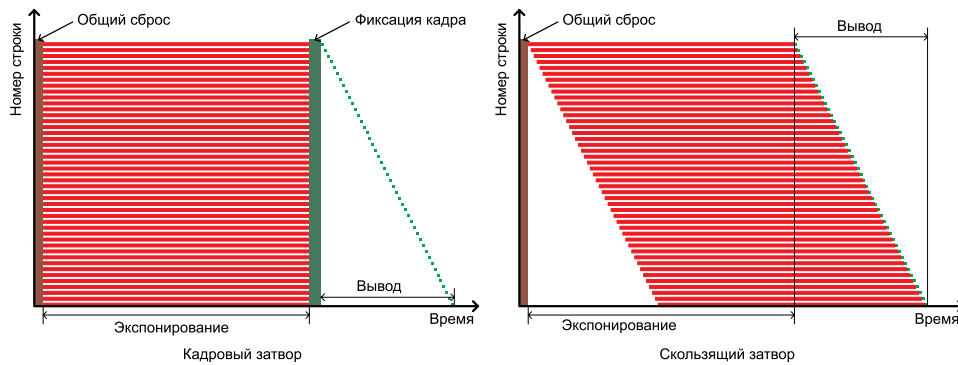


Рис. 1. Принцип формирования изображения при кадровом и скользящем затворах

3. Часто приводится соотношение «Сигнал/Шум», но существует несколько методик его расчета. Сравнивать этот параметр для изделий различных производителей довольно рискованно.

Ряд параметров не имеет прямого отношения к фотоэлектронике, но при первом знакомстве может вызвать вопросы:

1. **Оптический формат в дюймах.** Общеизвестно, что ПЗС- или КМОП-датчик с размерами 2,4*3,2 мм (диагональ 4 мм) называют «1/4 inch», хотя в реальности четверть дюйма это 6,35 мм. Аналогично матрицы с диагоналями 6, 8, 11 и 16 мм называются, соответственно, треть, половина, две трети дюйма и дюйм. В реальности это не так и даже коэффициенты пропорциональности не всегда совпадают. Важно помнить: «две трети дюйма» — это не физический размер, а название определенного типа матриц. Соответствие реальных размеров и названий можно найти в источнике [2].

2. **Оптический формат 35 мм.** Напомним, что во времена пленочной фотографии наиболее распространенная фотопленка имела ширину 35 мм. Наиболее популярный размер кадра имел по ширине 24 мм и в длину 36 мм (были и другие варианты, но они имели, по крайней мере, один размер 24 мм и размещались на той же пленке). Применительно к ПЗС- и КМОП-датчикам, «формат 35 мм» обозначает, что один или оба размера чувствительной области матрицы равны 24 мм. Опять же «35 мм» — это не физический размер, а название класса изделий.

3. **Размер изображения** для монохромных и цветных матриц. Сама матрица изображения (то есть, массив фотоэлементов, размещенных на кристалле) является монохромной. Цветной она становится, если в процессе изготовления между кристаллом и микролинзами устанавливается светофильтр для каждой ячейки. Две из каждых четырех ячеек становятся «зелеными», одна «синей» и одна «красной». При этом упускается из виду, что каждый пиксель цветного изображения образован четырьмя ячейками на матрице. Следовательно, полное изображение, считанное, например, с монохромного варианта

датчика LUPA-1300-2 при отображении на экране монитора будет иметь размер 1280*1024, а полное изображение, считанное с цветного варианта датчика LUPA-1300-2, на мониторе будет иметь размер 640*512.

Особенности архитектуры КМОП-датчиков изображения ON Semiconductor. Варианты реализации электронного затвора

Применительно к КМОП-датчикам различают два способа формирования изображения на кристалле или, что то же самое, два вида электронных затворов: Global Shutter и Rolling Shutter. В русскоязычных источниках первый термин переводится как «кадровый затвор» (реже — «глобальный» или «моментальный»). Второй термин переводится как «скользящий затвор» (реже — «последовательный»). В Global Shutter изображение на кристалле формируется одновременно для всех элементов изображения (пикселей, столбцов, строк). Свет накапливается в течение определенного времени экспонирования, но моменты начала и конца экспонирования едины для всей матрицы. В пленочной фотографии наиболее близким аналогом кадрового затвора является так называемый центральный затвор [3]. В Rolling Shutter изображение формируется не одновременно, а последовательно по строкам. Заметим, экспонирование осуществляется не строго построчно — одна строка за другой, а параллельно-последовательно — моменты начала экспонирования для соседних строк «стартуют» один за другим, а интервалы экспонирования соседних строк перекрываются. Для любых строк время экспонирования одинаково, но моменты начала и окончания экспонирования смещены «сверху — вниз». В пленочной фотографии наиболее близким аналогом является штормый фокальный затвор [3]. Различия в принципе формирования изображения иллюстрируются рисунком 1. Считается, что смазывание изображения при фотографировании движущихся объектов характерно только для скользящего затвора. В действительности при про-

должительном времени экспонирования смазывание возникнет при затворе любого типа. И в кадровом, и в скользящем затворе этот эффект проявляется по горизонтали, например, в случае движения объекта фотографирования. Но в скользящем затворе, кроме того, возникнет смазывание и по вертикали, как следствие разновременности моментов экспонирования от верхних к нижним строкам. При фотографировании неподвижных изображений оба затвора дадут одинаковый результат. Кадровый затвор в КМОП-датчиках изображения применяется достаточно редко — как правило, только в тех случаях, когда объектами съемки являются быстро изменяющиеся сцены. Реализация скользящего затвора существенно проще, и конечное изделие, как следствие, оказывается дешевле. Для большинства приложений погрешность, вносимая скользящим затвором, не представляет существенной, и поэтому в КМОП-датчиках изображения реализован, как правило, скользящий затвор. В линейке компании ON Semiconductor кадровый затвор реализован только в семействах VITA и LUPA (хотя и в них заложен режим Rolling Shutter). В семействах STAR и IBIS реализован только скользящий затвор.

Кадровый затвор в изделиях ON Semiconductor реализован в двух модификациях: конвейерном (pipelined) и триггерном (triggered). В конвейерном режиме формирование очередного кадра и считывание предыдущего происходит параллельно. Каждый кадр начинается с временного интервала FOT (Frame Overhead Time — «добавленное время кадра»), в течение которого аналоговая величина на зарядном конденсаторе ячейки пикселя перезаписывается в ее запоминающий элемент. После этого заряд на конденсаторе сбрасывается и на нем вновь начинается накопление заряда (но это уже значение со следующего кадра). Считывание данных с запоминающего элемента происходит одновременно, последовательно, строка за строкой. На рисунке 2 представлена временная диаграмма конвейерного режима. Триггерный режим матрицы — это режим ожидания, работа начинается по внешнему сигналу. Сначала происходит формирование изображения, а затем его считывание, после чего матрица вновь переходит в дежурный режим. Строго говоря, при определенной частоте сигналов запуска формирование нового кадра и считывание предыдущего могут накладываться друг на друга без потерь кадров, но эта ситуация является частным случаем. Конвейерный режим в общем случае предназначен для формирования видеопоследовательности кадров, а триггерный — для одиночной съемки (то есть, фотографирования).

На рисунке 3 представлена временная диаграмма триггерного режима.

И в конвейерном, и в триггерном режиме существуют две модификации — ведущего (Master) и ведомого (Slave) устройств. В состоянии ведущего устройство работает автономно, время экспозиции определяется установками внутренних регистров, а начало экспонирования — внутренним генератором (в конвейерном режиме) или внешним сигналом (в триггерном). В состоянии ведомого устройства матрица работает по внешнему сигналу: его фронт начинает процесс формирования кадра, а его продолжительность определяет время экспонирования. Этот режим применяется при необходимости совместной и согласованной работы устройства, содержащего два и более КМОП-датчиков изображения. Примером таких устройств являются цифровые фотоаппараты для аэро- и космической фотосъемки, где изображение формируется одновременно на значительном количестве датчиков.

Режим скользящего затвора по функциональности эквивалентен триггерному режиму ведущего устройства, с той разницей, что запуск может осуществляться как по внешнему сигналу, так и от внутреннего генератора (в зависимости от установок программно доступных регистров).

Особенности архитектуры КМОП-датчиков изображения ON Semiconductor. Режимы фрагментирования изображения

Режим фрагментирования является характерным отличием именно КМОП-матриц, поскольку в ПЗС-матрицах он не может быть реализован принципиально. Под фрагментированием или кадрированием (windowing), понимается вывод с матрицы не полного изображения, а только некоторого его подмножества. Во всех КМОП-датчиках компании ON Semiconductor реализованы, как минимум, три режима: **нормальный** (Normal) режим считывания полного изображения, **прореживание** (Subsampling) и, собственно, **фрагментирование** (ROI — Region of Interest). Прореживание предполагает вывод не каждого пикселя, а одного из четырех (а также 1 из 9, 1 из 16, 1 из 36 и т.д., в зависимости от функций конкретного устройства). То есть на вывод подается только пиксель с каждого второго (3-го, 4-го или 6-го) столбца каждой второй (3-ей, 4-ой или 6-ой) строки. Остальные три (8, 15 или 35) пикселей окрестности игнорируются. Режим прореживания иллюстрируется рисунком 4. Фрагментирование предполагает вывод с матрицы только фрагмента $m \times n$ пикселей (из m строк и n столбцов) с началом в точке $(x; y)$. Размеры и расположение фрагмента могут быть произвольными. Области исходного изображе-

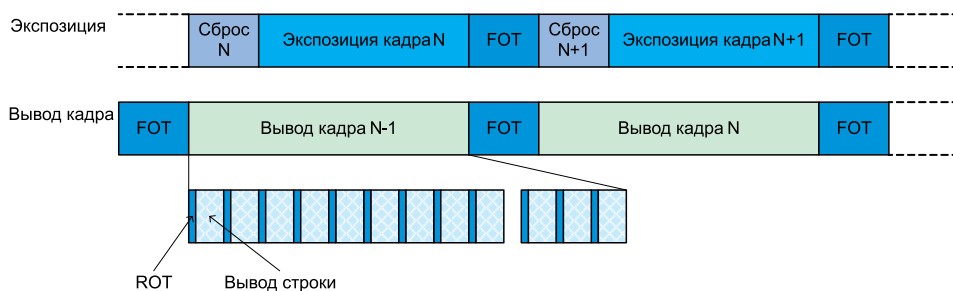


Рис. 2. Временная диаграмма конвейерного режима (Master)

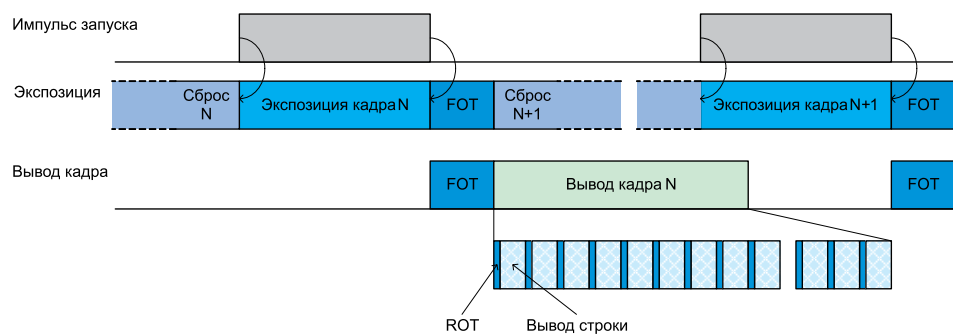


Рис. 3. Временная диаграмма триггерного режима (Master)

ния, не попавшие в заданный фрагмент, игнорируются и на вывод не подаются. В датчиках семейства VITA, а также в издании LUPA-1300-2, реализован мультиоконный режим фрагментирования, при котором имеется возможность осуществлять параллельный вывод не одного фрагмента, а нескольких (до 32 в издании VITA-25K). С конкретными особенностями задания мультиоконного режима и оригинальным механизмом формирования выходной последовательности можно ознакомиться в материалах компании ON Semiconductor, например [4].

Для чего необходимы режимы фрагментирования

Приведем три примера, когда данная функция дает ощутимые преимущества. Во-первых, при высокоскоростной видеосъемке (серия LUPA) прореживание «один к четырем» даст уменьшение объема сброшенной информации в четыре раза, что позволит обеспечить ка-

дровую частоту до значений, близких к 2000 кадров в секунду. Однако, следует иметь в виду, что при этом снижается время экспонирования матрицы и может оказаться, что условия освещенности не позволят сформировать качественное изображение. Второе применение: перед осуществлением видео- или фотосъемки осуществляется выбор режима экспонирования. В идеале, для качественного отображения деталей необходимо, чтобы самые темные участки фотографируемого объекта были экспонированы на уровне, близком к уровню темнового тока (уровень черного), самые светлые — на уровне, близком к уровню насыщения ячейки (уровень белого), а средняя освещенность по кадру — на середине динамического диапазона (уровень серого). Все три точки привязать невозможно, поэтому на практике фиксируют две из трех (конкретный выбор зависит от желаемого результата). При этом в расчет может браться все изо-

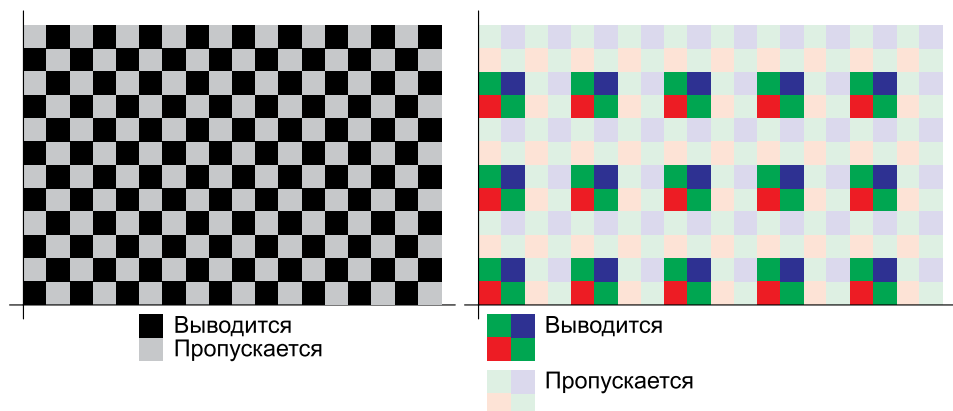


Рис. 4. Прореживание изображения как режим фрагментирования

бражение (так называемый режим интегральной экспозиции) или некоторый, наиболее значимый, фрагмент (режим дифференциальной или фрагментарной экспозиции). Для расчета не требуется вывод всего изображения целиком, поскольку большой объем данных увеличивает и время расчета. Для интегрального режима удобным оказывается расчет по прореженному изображению, а в дифференциальном режиме — по заданному фрагменту. И наконец, как отмечалось выше, мультиоконное фрагментирование позволяет существенным образом упростить решение задачи отслеживания нескольких движущихся объектов на фоне неподвижного изображения.

Системы биометрической идентификации как потенциальная область применения датчика IBIS4-6600

Системы контроля доступа принято разделять на три группы в зависимости от способа, которым человек подтверждает свое право доступа:

1. **Парольная защита.** Пользователь предъявляет данные, которые, как предполагается, известны только ему (например, PIN-код или пароль).

2. **Использование ключей.** Пользователь предъявляет свой персональный идентификатор, являющийся физическим носителем секретного цифрового кода. Таким идентификатором могут являться магнитные карты, контактные или бесконтактные смарт-карты.

3. **Биометрия.** Пользователь предъявляет параметр, который является частью его самого. То есть, идентификации подвергаются индивидуальные особенности сетчатки или радужной оболочки глаза, отпечатка пальцев, распознавание голоса и т.д.

Достоинства биометрической идентификации

Пароль можно забыть, а записную книжку с его записью потерять. Ключ может быть потерян, украден или скопирован. Биометрический параметр связан с конкретной частью тела человека, он постоянно находится «при себе» и потерять его можно только в результате получения увечья. Существенное отличие: биометрический идентификатор невозможно передать третьим лицам.

Рассмотрим основные методы биометрической идентификации, связанные с анализом изображений в видимой части спектра:

1. По отпечатку пальца.
2. По изображению сетчатки глаза.
3. По рисунку радужной оболочки глаза.

Идентификация по отпечатку пальца в настоящее время наиболее распространенный метод. Это связано не столько с особыми достоинствами распознавания, сколько с наличием достаточно прорабо-

танной теории, доставшейся от криминалистики. Метод дает вполне удовлетворительные показатели как по вероятности «ложной тревоги», так и по вероятности «пропуска тревоги». Некоторое неприятие идентификации по отпечатку пальца вызывает устоявшаяся взаимосвязь термина с криминалистикой и, следовательно, криминалом. Более того, не каждому даже законопослушному человеку понравится тот факт, что изображение отпечатка его пальца останется в распоряжении, например, бывшего работодателя. Эксперты в области биометрической идентификации [5] предполагают, что именно эти обстоятельства приведут к замене отпечатков пальца на более «политкорректные» процедуры идентификации — по изображению сетчатки или радужной оболочки глаза. Идентификация по сетчатке глаза предполагает анализ рисунка кровеносных сосудов глазного дна, которое уникально для каждого человека, хотя и несколько изменяется с возрастом. Рисунок радужной оболочки (текстура, содержащая множество колец, кругов и микрорисунков) также уникален. Но, кроме того, он не меняется с возрастом, а анализ радужной оболочки инвариантен к наличию контактных линз. Оба метода дают, как минимум, на десятичный порядок лучшие показатели «ложной тревоги» и «пропуска тревоги» по сравнению с анализом отпечатка пальца.

Строго говоря, нас интересуют не столько достоинства и недостатки различных методов биологической идентификации, сколько совокупность технических требований, которые предъявляют эти методы к параметрам датчиков изображения. В большинстве сканеров отпечатка пальца используется монохромный датчик изображения с размером 1...3 мегапикселя. Современные алгоритмы распознавания отпечатков пальцев используют 30...70 так называемых характерных точек, или, если точнее, небольших фрагментов. Системы идентификации по сетчатке или радужной оболочке глаза позволяют выделить и использовать при распознавании порядка 200...270 характерных точек. Соответственно, и размер изображения, получаемого с датчика, в несколько раз больше и лежит в пределах 4...10 мегапикселей. Алгоритмы распознавания не используют информацию о цвете, следовательно, оправдано только применение монохромных датчиков. Как правило, фиксируется неподвижное изображение: клиент смотрит в «глазок». Соответственно, нет необходимости в применении кадрового затвора, могут использоваться более простые датчики со скользящим затвором. Высокая чувствительность не требуется, поскольку, как правило, применяется боковая подсветка. Высокая частота кадров также не требуется, поскольку анализируется один, в спорных случаях — несколько снимков.

Скорость съема данных с матрицы также не является критичной, поэтому обмен по CMOS-интерфейсу предпочтителен: упрощается «приемная» часть, а, следовательно, снижается цена конечного изделия. Датчик IBIS4-6600 отвечает всем без исключения требованиям, указанным выше. Более того, дополнительные возможности, например, возможность фрагментирования, тоже могут быть задействованы, поскольку алгоритм распознавания основан именно на работе с фрагментами. Неиспользуемых функций датчика практически не остается.

Заключение

Номенклатура КМОП-датчиков от ON Semiconductor состоит из чуть более 20 изделий, включая варианты исполнения. Однако, реальные функциональные возможности уже существующих изделий ON Semiconductor покрывают не только потребности универсальных датчиков изображения, но и достаточно узкие и специализированные ниши, как например, высокоскоростная съемка, мониторинг движущихся объектов, астрономическая съемка.

Применительно к системам безопасности значительный интерес представляет биометрическая идентификация в системах контроля доступа. В этом плане IBIS4-6600 является оптимальным решением. Семейства VITA и LUPA могут найти применение в сфере обеспечения безопасности промышленных производств как высокотехнологичные элементы систем технического зрения.

Все упоминаемые в статье изделия поставляются только под заказ.

Литература

1. Майоров В.П., Овчинников Л.Ф., Семин М.С. Рассуждения о телевизионных камерах // Компьютерра, №14, 1998. Страница в Интернете: <http://www.videoscan.ru/page/692>.
2. ПЗС-матрица. (Статья в Википедии). Страница в Интернете: <http://ru.wikipedia.org/wiki/ПЗС-матрица>.
3. Фотокинотехника: Энциклопедия // под редакцией Е. А. Иофиса. — М.: Советская энциклопедия, 1981.
4. VITA 2000 2.3 Megapixel 92 FPS Global Shutter CMOS Image Sensor. Материал компании On Semiconductor. Размещение в Интернете: <http://www.onsemi.ru.com/pub/Collateral/NOIV1SN2000A-D.PDF>.
5. Морзеев Ю. Современные биометрические решения в системах безопасности // Статья на сайте www.r-control.ru. Страница в Интернете: <http://www.r-control.ru/articles/article4>.

Получение технической информации,
заказ образцов, поставка —
e-mail: sensors.vesti@compel.ru