2016 №10

ЭТ

Компоненты для систем безопасности и защиты данных

www.compel.ru

НОВОСТИ ЭЛЕКТРОНИКИ

№10 (156), 2016 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
Александр Маргелов
Николай Паничкин
Борис Рудяк

Дизайн, графика, верстка:
Елена Георгадзе
Евгений Торочков

E-mail-рассылка и продвижение:
Снежана Холодова
Екатерина Железнова
Александра Гирина

Электронная подписка:
www.compel.ru/mail

Распространяется бесплатно в электронном виде

Подписано к публикации:
9 ноября 2016 г.

СОДЕРЖАНИЕ

ТЕМА НОМЕРА: КОМПОНЕНТЫ ДЛЯ СИСТЕМ БЕЗОПАСНОСТИ

МИКРОКОНТРОЛЛЕРЫ

БЕСПРОВОДНЫЕ ТЕХНОЛОГИИ

life.augmented

TEXAS INSTRUMENTS

В СКОРО: ВЫПУСК ЖУРНАЛА, ПОСВЯЩЕННЫЙ КОМПОНЕНТАМ ДЛЯ БЕСПРОВОДНЫХ СИСТЕМ

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!

Какой бы теме ни был посвящен номер «Новостей электроники» в этом году, большинство редакционных заметок так или иначе сводится к теме беспроводной связи, «умного дома» и Интернета вещей (IoT). И тут уж ничего не поделаешь — это, как принято сейчас выражаться, тренд. Когда-то в начале своего развития таким трендом было светодиодное освещение. Затем ажиотаж на эту тему поутих, минусы уравновесили плюсы, технология стала развиваться своим чередом - спокойно, без бурных всплесков. Возможно, и тема децентрализованной управляющей беспроводной сети, завоевав приличную часть рынка, уйдет из раздела «горячие новости» и станет спокойно развиваться. Однако сама эта технология затрагивает гораздо более глубокие основы организации жизни и, следовательно, более важна.

А уж рынок систем безопасности эта тема затрагивает, может быть, больше, чем иные области. Сеть контроля передачи данных, сеть управления физическим доступом, сеть автоматического пожаротушения с предупреждением всем подразделениям о временном перераспределении производственных мощностей и административных функций — это лишь некоторые примеры.

К тому же, наше государство не дает угаснуть различным отраслям электроники, время от времени принимая различные законы, стимулирующие их развитие. Не так давно это были законы об усилении учета и контроля за расходом электроэнергии и других возобновляемых ресурсов. Оживились производители электросчетчиков и счетчиков воды, был освоен выпуск новых моделей с возможностью дистанционного беспроводного сбора данных. Следующим был пакет законов и подзаконных актов, посвященных контролю и учету движения транспорта. Теперь практически все транспортные средства страны оснащены приемопередатчиками системы ГЛОНАСС, а на орбите размещена полномасштабная группировка навигационных спутников. А недавно в России принят пакет антитеррористических законов, который, в частности, вносит поправки в закон «О связи». Теперь три года будет храниться информация о фактах приема и передачи звуковых, текстовых и видеосообщений, а само содержание переговоров и переписки — полгода. Причем все эти данные должны храниться и обрабатываться внутри страны. Средства сетевого мониторинга и анализаторы трафика придется закупать за рубежом — в России оборудование этой группы и нужных класса и мощности попросту не производится. А вот строить новые центры обработки и хранения данных для размещения оборудования придется в России. Эксперты утверждают, что к 2020 году рынок коммерческих центров обработки данных (ЦОД) может вырасти примерно на 15 тысяч стоек. А что такое новые дата-центры? Это, помимо закупки, установки и наладки оборудования, еще и вся инженерная инфраструктура: бесперебойное питание и освещение, телекоммуникационная и информационная безопасность, система автоматического газового пожаротушения, удаленный IP-контроль и многоуровневый контроль физического доступа. И все это должно обладать максимальным уровнем не только вертикального, но и горизонтального взаимодействия и резервирования функций.

Понятно, что отечественные производители соответствующего оборудования встретили новый пакет законов с энтузиазмом. Однако основная элементная база для создания отечественных систем безопасности все равно поставляется из-за рубежа. И компания КОМПЭЛ умеет поставлять эти компоненты, а также сопровождать проекты и оказывать инженерную поддержку разработчикам. Обращайтесь к нам!

С уважением,
Геннадий Каневский

Вячеслав Гавриков (г. Смоленск)

ШИФРОВАНИЕ ДАННЫХ: КРИПТОЗАЩИТА STM32

*С развитием таких сетевых технологий как **Интернет вещей,** вопросы безопасного обмена данными становятся все более важными. Чтобы помочь своим потребителям в создании защищенных приложений, компания **STMicroelectronics** выпустила программный пакет **X-CUBE-CRYPTOLIB.** В нем содержатся библиотеки, которые реализуют наиболее популярные **алгоритмы защиты данных** для всех семейств **микроконтроллеров STM32,** даже для тех, которые не имеют в своем составе аппаратных блоков криптографии.*

Существует огромное количество приложений, которые по определению должны обеспечивать высокую степень защиты данных. Это касается Интернета вещей (IoT), терминалов оплаты, банкоматов, счетчиков коммунальных услуг, систем безопасности и многих других. При этом в каждом из перечисленных случаев необходимо защитить данные не только от кражи, но и от вредоносного изменения. Это достаточно сложная задача.

Часть разработчиков IoT-устройств пока даже не задумывается о мерах безопасности. Можно лишь надеяться, что эта беспечность рано или поздно не приведет к плачевным последствиям. С другой стороны, создание механизмов защиты — сложное и затратное мероприятие, и не у каждой компании найдутся для этого ресурсы. В этих условиях спасает то, что крупные производители процессоров и микроконтроллеров стремятся в той или иной форме обеспечить своих потребителей инструментами для создания безопасных приложений. Яркий пример — новый программный пакет X-CUBE-CRYPTOLIB от **STMicroelectronics.**

В июле 2016 года компания STMicroelectronics сообщила, что ее фирменная библиотека шифрования, входящая в состав X-CUBE-CRYPTOLIB, успешно прошла сертификацию в соответствии с требованиями US Cryptographic Algorithm Validation Program (CAVP). Библиотека состоит из двух частей: аппаратно зависимой, для контроллеров с интегрированными блоками шифрования, и аппаратно независимой, для контроллеров, в которых интегрированные аппаратные блоки отсутствуют. Сам пакет X-CUBE-CRYPTOLIB является программным расширением хорошо знакомой программистам системы **STM32Cube.**

Библиотека шифрования имеет сертифицированную поддержку следующих алгоритмов:

- AES-128, AES-192, AES-256 (ECB (*Electronic Codebook Mode*), CBC (*Cipher-Block Chaining*), CTR (*Counter Mode*), CFB (*Cipher Feedback*), OFB (*Output Feedback*), CCM (*CBC-MAC*), GCM (*Galois Counter Mode*), CMAC, KEY WRAP, XTS);
- хеш-функции с поддержкой HMAC (SHA-1, SHA-224, SHA-256, SHA-384, SHA-512);
- программный генератор случайных чисел на базе DRBG-AES-128;
- RSA с PKCS#1v1.5 (кодирование/декодирование, цифровые подписи);
- ECC (*Elliptic Curve Cryptography*) — генерация ключей, Scalar multiplication, ECDSA.

Кроме того, библиотека имеет несертифицированную поддержку дополнительных алгоритмов ARC4, DES, TripleDES (ECB (*Electronic Codebook Mode*) и CBC (*Cipher-Block Chaining*)), хеш-функции (MD5 и HKDF-SHA-512), ChaCha20, Poly1305, CHaCHA20-POLY1305, ED25519, Curve25519.

Библиотека представляет собой набор скомпилированных файлов, предназначенных для работы с конкретными семействами контроллеров и разработки (IDE). К услугам программистов предлагаются скомпилированные версии для всех семейств STM32 и наиболее популярных систем — Keil® MDK-

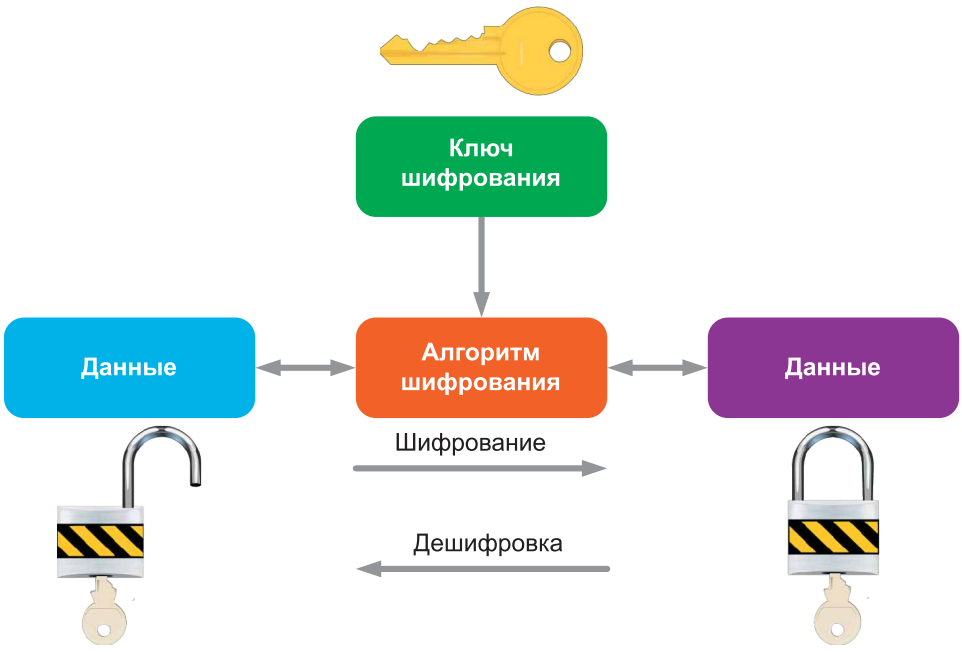


Рис. 1. **Механизм шифрования данных**

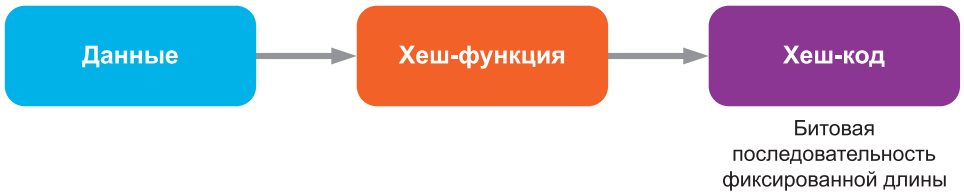


Рис. 2. **Работа хеш-функций**

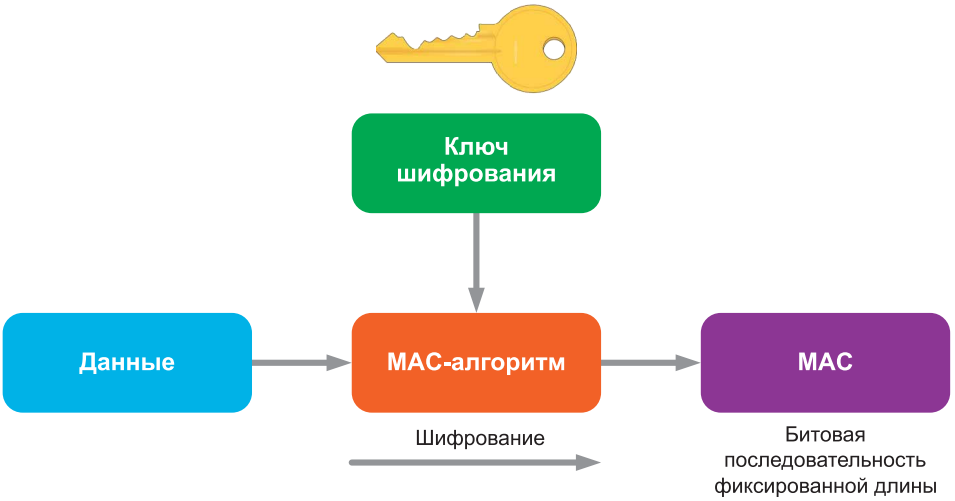


Рис. 3. **Механизм работы MAC- алгоритмов**

ARM™, IAR Embedded Workbench® EWARM, IDE на базе GCC, например, SW4STM32 и Atollic® TrueSTUDIO®.

Обзор основных методов защиты данных

Проблему защиты данных можно разделить на несколько задач [1].

Сохранение целостности информации подразумевает защиту от несанкционированного или случайного искажения данных. Под искажением понимают удаление, изменение или вставку сторонней информации в защищаемый блок данных. Чтобы обезопасить себя от подобных воздействий, система должна иметь возможности их обнаружения, то есть приемник, получив блок данных, должен убедиться, что они не были изменены.

Конфиденциальность подразумевает, что доступ к закрытым данным могут иметь только авторизованные пользователи. Доступ неавторизованных пользователей или процессов должен быть исключен.

Идентификация и аутентификация позволяют сторонам, участвующим в обмене данными, идентифицировать себя. Если аутентификация проходит успешно, пользователь или процесс получают доступ к информации. Аналогично есть необходимость идентификации источника данных.

Безотказность. Согласно ГОСТ Р ИСО 7498-2-99, этот метод может принимать две формы [2].

Безотказность с подтверждением отправителя подразумевает, что получатель данных обеспечивается проверкой отправителя данных. Это защищает от любой попытки отправителя ложно отрицать передачу данных или их содержимое.

Безотказность с подтверждением доставки гарантирует, что передатчик данных обеспечивается подтверждением доставки данных. Это защищает от любой последующей попытки получателя ложно отрицать получение данных или их содержимое.

Очевидно, что проблема защиты данных вовсе не нова. На настоящий момент существуют надежные и проверенные функции и методы обеспечения безопасности. Все они необходимы для решения перечисленных подзадач [1].

Шифрование. Суть этого метода заключается в преобразовании открытых данных в зашифрованную форму (рисунок 1). Кодирование производится с помощью специальных алгоритмов и ключа шифрования. Обратный процесс декодирования также требует ключа. При этом возможно два варианта. При симметричном шифровании для кодирования и декодирования используется один и тот же ключ. При асимметричном шифровании для кодирования используется один ключ, а для декодирования – другой.

Функции хеширования (свертки) – это особый вид односторонних функций, которые с помощью определенного алгоритма получают из исходного массива данных битовую строку заданной длины (рисунок 2). Исходные данные часто называют ключом (сообщением), а выходную битовую строку «хеш-кодом», «хеш-суммой» или «сводкой сообщения». Используемый алгоритм преобразования должен обеспечивать защиту от возможностей восстановления исходных данных по известному хеш-коду и совпадения хеш-кодов разных сообщений.

Код аутентификации сообщений MAC (*Message Authentication Code*). Данный механизм, как и хеш-функции, используется для генерации хеш-кода. Однако для этого требуется не только исходное сообщение, но и секретный ключ, известный только отправителю и получателю (рисунок 3). Это позволяет получателю данных проверять целостность информации и идентифицировать отправителя. Если отправитель не имеет секретного ключа – хеш-код будет сформирован неверно, что легко обнаружит получатель.

Цифровые подписи. Этот механизм позволяет производить аутентификацию сообщений, то есть доказывать их подлинность с помощью цифровой подписи. Цифровая подпись работает практически так же, как и обычная подпись на бумаге – по ней всегда можно распознать отправителя. При получении цифровой подписи применяют ассимме-

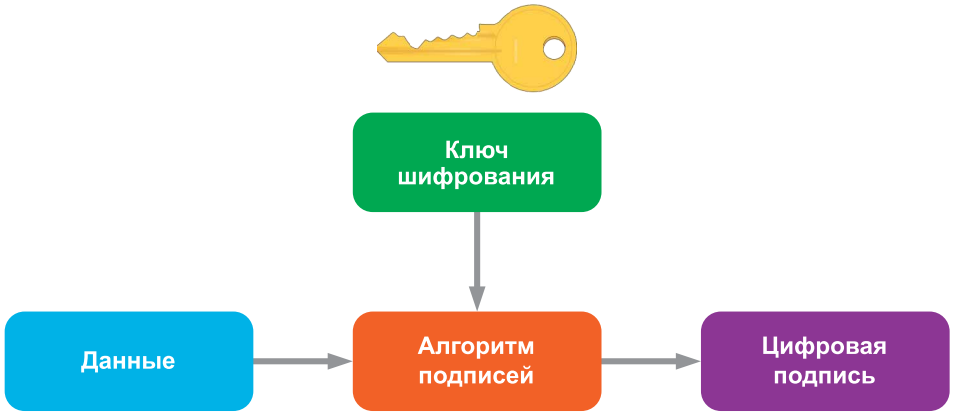


Рис. 4. **Механизм формирования цифровых подписей**

Таблица 1. **Методы защиты информации**

Метод	Контроль целостности данных	Конфиденциальность	Идентификация и аутентификация	Безотказность
Симметричное шифрование	Нет	да	нет	нет
Защищенные хеш-функции	Да	нет	нет	нет
MAC	Да	нет	да	нет
Цифровые подписи	Да	нет	да	да

Таблица 2. **Варианты компиляции аппаратно-независимой библиотеки шифрования**

Семейство	Компилятор	Оптимизация	Библиотека
STM32F0	IAR	Скорость	STM32CryptographicV3.0.0_CM0_IAR_ot.a
		Размер	STM32CryptographicV3.0.0_CM0_IAR.a
	KEIL	Скорость	STM32CryptographicV3.0.0_CM0_KEIL_otslsm1elfspf.lib
		Размер	STM32CryptographicV3.0.0_CM0_KEIL_slsm1elfspf.lib
	GCC	Скорость	STM32CryptographicV3.0.0_CM0_GCC_ot.a
		Размер	STM32CryptographicV3.0.0_CM0_GCC.a
STM32L0	IAR	Скорость	STM32CryptographicV3.0.0_CM0PLUS_IAR_ot.a
		Размер	STM32CryptographicV3.0.0_CM0PLUS_IAR.a
	KEIL	Скорость	STM32CryptographicV3.0.0_CM0PLUS_KEIL_otslsm1elfspf.lib
		Размер	STM32CryptographicV3.0.0_CM0PLUS_KEIL_slsm1elfspf.lib
	GCC	Скорость	STM32CryptographicV3.0.0_CM0PLUS_GCC_ot.a
		Размер	STM32CryptographicV3.0.0_CM0PLUS_GCC.a
STM32F1, STM32F2, STM32L1	IAR	Скорость	STM32CryptographicV3.0.0_CM3_IAR_ot.a
		Размер	STM32CryptographicV3.0.0_CM3_IAR.a
	KEIL	Скорость	STM32CryptographicV3.0.0_CM3_KEIL_otslsm1elfspf.lib
		Размер	STM32CryptographicV3.0.0_CM3_KEIL_slsm1elfspf.lib
	GCC	Скорость	STM32CryptographicV3.0.0_CM3_GCC_ot.a
		Размер	STM32CryptographicV3.0.0_CM3_GCC.a
STM32F3, STM32F4, STM32L4	IAR	Скорость	STM32CryptographicV3.0.0_CM4_IAR_ot.a
		Размер	STM32CryptographicV3.0.0_CM4_IAR.a
	KEIL	Скорость	STM32CryptographicV3.0.0_CM4_KEIL_otslsm1elfspf.lib
		Размер	STM32CryptographicV3.0.0_CM4_KEIL_slsm1elfspf.lib
	GCC	Скорость	STM32CryptographicV3.0.0_CM4_GCC_ot.a
		Размер	STM32CryptographicV3.0.0_CM4_GCC.a
STM32F7	IAR	Скорость	STM32CryptographicV3.0.0_CM7_IAR_ot.a
		Размер	STM32CryptographicV3.0.0_CM7_IAR.a
	KEIL	Скорость	STM32CryptographicV3.0.0_CM7_KEIL_otslsm1elfspf.lib
		Размер	STM32CryptographicV3.0.0_CM7_KEIL_slsm1elfspf.lib

триченое шифрование (рисунок 4). Для шифрования сообщения используется закрытый ключ, а для расшифровки – открытый. Закрытый ключ известен только отправителю, в то время как к открытому ключу доступ может иметь множестов получателей данных.

Генерация случайных чисел. Защитное кодирование имеет смысл, только если невозможно разгадать ключ шифрования. По этой причине ключ должен быть случайным. Для этого применяется генератор случайных чисел (рисунок 5). Он может использовать как программные методы формирования исходной последовательности случайных чисел, так и естественный источник случайного сигнала, например, шум напряжения на диоде.

Если проанализировать задачи защиты данных, то окажется, что для реализации каждой из них может потребоваться несколько различных механизмов (таблица 1).

Пакет расширения X-CUBE-CRYPTOLIB для STM32 Cube

Для разработки устройств на базе микроконтроллеров семейства **STM32** производства компании STMicroelectronics создана целая экосистема – программно-аппаратная платформа **STM32 Open Development Environment** (STM32 ODE). STM32 ODE объединяет аппаратные инструменты и программные библиотеки, которые, в свою очередь, организованы в виде единого комплекса STM32 Cube. К аппаратной части относятся автономные отладочные наборы (*Evaluation boards*), стартовые наборы (*Discovery boards*), базовые платы

Рис. 5. **Пример работы генератора случайных чисел**

Таблица 3. **Варианты компиляции аппаратно-зависимой библиотеки шифрования**

Семейство	Наименование	Поддерживаемые алгоритмы шифрования	Используемый аппаратный блок
STM32F2	STM32F20x	ECC: генерация ключей, скалярное умножение, ECDSA	Генератор случайных чисел (RNG)
		RSA функции шифровки/дешифровки с использованием PKCS#1v1	
	STM32F21x	AES: CFB, OFB, XTS, CCM, GCM, CMAC, KeyWrap; разрядность ключа: 128, 192, 256 бит	Блок шифрования (Crypto accelerator)
		ECC: генерация ключей, скалярное умножение, ECDSA	Генератор случайных чисел (RNG)
		RSA функции шифровки/дешифровки с использованием PKCS#1v1.5	
STM32F4	STM32F405/407	ECC: генерация ключей, скалярное умножение, ECDSA	Генератор случайных чисел (RNG)
	STM32F427/429	RSA: функции шифровки/дешифровки с использованием PKCS#1v1	
	STM32F415x/417x	AES: CFB, OFB, XTS, CCM, GCM, CMAC, KeyWrap; разрядность ключа: 128, 192, 256 бит	Блок шифрования (Crypto accelerator)
		ECC: генерация ключей, скалярное умножение, ECDSA	Генератор случайных чисел (RNG)
		RSA функции шифровки/дешифровки с использованием PKCS#1v1.5	
	STM32F437x/439x	AES: CFB, OFB, XTS, CCM, GCM, CMAC, KeyWrap; разрядность ключа: 128, 192, 256 бит	Блок шифрования (Crypto accelerator)
		ECC: генерация ключей, скалярное умножение, ECDSA	Генератор случайных чисел (RNG)
		RSA функции шифровки/дешифровки с использованием PKCS#1v1.5	
STM32F7	STM32F745x/746x	ECC: генерация ключей, скалярное умножение, ECDSA	Генератор случайных чисел (RNG)
		RSA функции шифровки/дешифровки с использованием PKCS#1v1.5	
	STM32F756xx	AES: CFB, OFB, XTS, CCM, GCM, CMAC, KeyWrap; разрядность ключа: 128, 192, 256 бит	Блок шифрования (Crypto accelerator)
		ECC: генерация ключей, скалярное умножение, ECDSA	Генератор случайных чисел (RNG)
		RSA функции шифровки/дешифровки с использованием PKCS#1v1.5	
STM32L0	STM32L05x	ECC: генерация ключей, скалярное умножение, ECDSA	Генератор случайных чисел (RNG)
		RSA функции шифровки/дешифровки с использованием PKCS#1v1.5	
	STM32L06x	AES: CFB, OFB, XTS, CCM, GCM, CMAC, KeyWrap; разрядность ключа: 128 бит	Блок шифрования (Crypto accelerator)
		ECC: генерация ключей, скалярное умножение, ECDSA	Генератор случайных чисел (RNG)
		RSA функции шифровки/дешифровки с использованием PKCS#1v1.5	
STM32L1	STM32L16x	AES: CFB, OFB, XTS, CCM, GCM, CMAC, KeyWrap; разрядность ключа: 128 бит	Блок шифрования (Crypto accelerator)
STM32L4	STM32L471xx	ECC: генерация ключей, скалярное умножение, ECDSA	Генератор случайных чисел (RNG)
		RSA функции шифровки/дешифровки с использованием PKCS#1v1.5	
	STM32L486xx	AES: CFB, OFB, XTS, CCM, KeyWrap; разрядность ключа: 128, 256 бит	Блок шифрования (Crypto accelerator)
		ECC: генерация ключей, скалярное умножение, ECDSA	Генератор случайных чисел (RNG)
		RSA функции шифровки/дешифровки с использованием PKCS#1v1.5	

(*Nucleo boards*) и платы расширения для Nucleo.

STM32 Cube — программная часть платформы STM32 ODE. Она объединяет ПО таких уровней как:

- уровень аппаратно зависимых драйверов (стандартная библиотека периферии);
- уровень аппаратно независимых драйверов для микроконтроллеров (*Hardware abstraction Layer*) и драйверы для плат расширения (B*oard support Package, BSP*);
- ПО промежуточного уровня Middleware (различные стеки протоколов, например, USB, Bluetooth и дополнительные библиотеки, например, рассматриваемая нами библиотека шифрования);
- ПО прикладного уровня, в основном, примеры для отладочных плат.

Пакет расширения для защищенных приложений X-CUBE-CRYPTOLIB входит в состав STM32 Cube (рисунок 6). Он включает программное обе-

спечение, работающее на двух уровнях: на уровне приложений и на промежуточном уровне.

ПО прикладного уровня. К услугам разработчиков предлагается 31 пример для каждого алгоритма защиты. Также здесь представлены шаблоны для наиболее популярных сред разработки (IAR, Keil ARM®, GCC) и шаблоны для различных аппаратных средств (отладочные наборы, стартовые наборы, платы Nucleo).

Все ПО этого уровня представлено в виде открытых файлов на языке С. Это значит, что пользователи с легкостью могут применять части кода в своих проектах, изменять и дополнять их, что позволяет максимально быстро освоить работу с библиотекой шифрования, которая функционирует на промежуточном уровне.

Библиотека шифрования STM32 crypto library представляет собой набор скомпилированных файлов для различных семейств микроконтроллеров и сред разработки. При этом каждый скомпилированный вариант реализации строится по модульному принципу. Такая структура позволяет компилятору использовать только те модули, которые нужны пользователю (AES CTR, AES CCM, HASH SHA, и так далее), а остальные, для экономии памяти, не включать в проект. Это также позволяет при необходимости добавлять модули в любой момент времени, как только это потребуется.

Так как библиотеки шифрования представлены в виде скомпилированных библиотечных файлов, то пользователи могут включать их в свои проекты, но не могут вносить в них изменения. По этой причине каждая библиотека поставляется в нескольких экземплярах: для каждой среды разработки (IAR, Keil ARM®, GCC) и с различными опциями, такими как оптимизация по скорости, оптимизация по объему памяти и так далее.

Обзор библиотеки шифрования STM32 crypto library из пакета расширения X-CUBE-CRYPTOLIB

Библиотека шифрования STM32 crypto library работает на промежуточном уровне (*Middlewares*) и доступна пользователям в виде большого количества скомпилированных файлов, которые объединены в две группы:

- аппаратно независимые версии (*Firmware implementation*) – версии, которые не используют специализированные аппаратные блоки шифрования, а потому способны работать со всеми микроконтроллерами STM32: от **STM32F0** до **STM32F7;**
- аппаратно зависимые ускорители (*Hardware acceleration*) – библиотеки-ускорители для микроконтроллеров STM32 со встроенными блоками шифрования. Наличие интегрированных модулей криптографии способно значительно ускорить работу приложений.

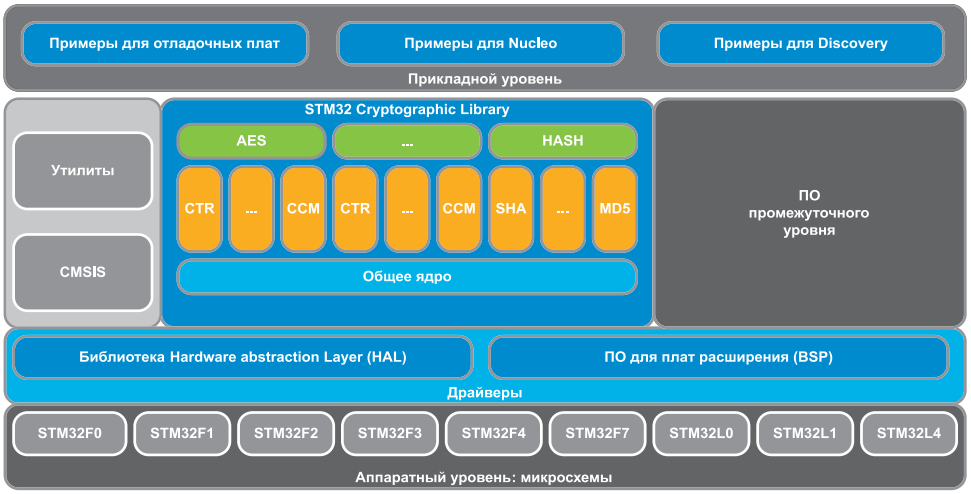


Рис. 6. **Положение библиотеки X-CUBE-CRYPTOLIB в системе ПО от STMicroelectronics**

При скачивании X-CUBE-CRYPTOLIB с сайта STMicroelectronics (*www.st.com*) пользователь получает архив STM32CubeExpansion_Crypto_V3.1.0. При его распаковке создается сложная сеть папок и вложенных директорий. Все файлы библиотеки шифрования, относящиеся к аппаратно зависимой части, находятся в папке AccHw_Crypto, а аппаратно независимые – в папке Fw_Crypto. Структура расположения файлов в этих директориях одинакова: для каждой серии STM32 (STM32F0, **STM32F1, STM32F2** и так далее) создана своя папка. При этом библиотеки поставляются в скомпилированном виде, поэтому для каждой версии предложено несколько вариантов, отличающихся используемым семейством микроконтроллеров, компилятором и видом оптимизации (по скорости, по занимаемому месту).

Выбор подходящего файла-библиотеки из пакета библиотек шифрования

При скачивании X-CUBE-CRYPTOLIB пользователь получает доступ к множеству различных скомпилированных библиотечных файлов:

- аппаратно независимых и аппаратно зависимых;
- созданных с помощью различных компиляторов (IAR, Keil ARM®, GCC);
- скомпилированных с различными установками оптимизации (по скорости, по объему занимаемой памяти).

Звучит это достаточно сложно, но в реальности такое решение оказывается вполне логичным. При этом выбор подходящего библиотечного файла делается за четыре шага.

- выбрать тип аппаратной реализации. Если применяемый микроконтроллер имеет встроенную специализированную периферию криптографии – следует использовать аппаратно зависимые библиотеки, если же это контроллер общего назначения – необходимо использовать аппаратно независимые реализации;
- необходимо выбрать группу библиотек в соответствии с семейством применяемого микроконтроллера;
- выбрать реализации алгоритма для своего компилятора (IAR, Keil ARM®, GCC);
- определиться с уровнем оптимизации конкретной скомпилированной версии библиотеки. На этом шаге стоит дать некоторые дополнительные пояснения.

Файлы аппаратно независимой библиотеки хранятся в отдельной директории “Middleware \ST\ STM32_Cryptographic\Lib” и имеют специальную систему именования: STM32CryptographicV3.0.0_CMx_C_O, где поля x, C и O кодируют информацию о файле:

- x – кодирует семейство микроконтроллеров: CM0 – STM32F0; CMPLUS – **STM32L0;** CM3 – STM32F1, STM32F2, **STM32L1;** CM4 – **STM32F3, STM32F4, STM32L4;** CM7 – STM32F7;
- C – кодирует тип компилятора: IAR, KEIL, GCC;
- O – кодирует тип оптимизации компилятора. (пусто) – оптимизация по размеру кода (для всех компиляторов); ot – оптимизация по скорости (для всех компиляторов); nsc – включена опция “No Size constraints” (только IAR); slsm – включена опция “Split Load и Store Multiple” (только для Keil); o1elfspf – включена опция “One ELF Section per Function” (только для Keil).

Всего пользователю доступно почти три десятка вариантов скомпилированной библиотеки шифрования (таблица 2).

Файлы аппаратно зависимых реализаций находятся в папке “Middleware\ST\STM32_Crypto_

Таблица 4. **Пример API библиотечных функций для реализации шифровавния AES**

Функция	Описание
AES_AAA_Encrypt_Init	Инициализация и загрузка ключа
AES_AAA_Encrypt_Append	Запуск операции шифрования
AES_AAA_Encrypt_Finish	Финализация процесса шифрования
AES_AAA_Decrypt_Init	Инициализация и загрузка ключа

AccHw\Lib". Их название имеет вид STM32AccHwCryptoV3.1.0_Xy_C_O.a. Поля xy, C и O также кодируют особенности файла.

- xy – кодирует семейство микроконтроллеров (STM32F2, STM32F4, STM32F7, STM32L0, STM32L1, STM32L4);
- C – кодирует тип компилятора: IAR, KEIL, GCC;
- O – кодирует тип оптимизации компилятора. (пусто) – оптимизация по размеру кода (для всех компиляторов); ot – оптимизация по скорости (для всех компиляторов); nsc – включена опция "No Size constraints" (только IAR); slsm – включена опция "Split Load и Store Multiple" (только для Keil); o1elfspf – включена опция "One ELF Section per Function" (только для Keil).

Всего доступно более десятка вариантов компиляции (таблица 3).

Таким образом, выбор подходящего скомпилированного файла библиотеки осуществляется за четыре шага. Несмотря на то, что библиотека является уже скомпилированной, следует отметить, что она не «съедает» память впустую, так как имеет модульную структуру. Это значит, что компиляторы автоматически помещают в память микроконтроллера только необходимые функции.

Перечень функций отдельных алгоритмов не отличается при использовании аппаратно зависимых и аппаратно независимых библиотек. Например, API для взаимодействия с AES AAA включает всего шесть функций для любого из вариантов реализации (таблица 4).

Кроме понимания того, как устроена библиотека, и как с ней работать, важно знать об особенностях лицензионного соглашения при использовании X-CUBE-CRYPTOLIB.

Лицензионное соглашение при использовании X-CUBE-CRYPTOLIB

Главное достоинство X-CUBE-CRYPTOLIB – пакет предоставляется бесплатно. Однако его использование связано с лицензионным соглашением [3], которое, впрочем, мало чем отличается от общей лицензии для аналогичных продуктов производства компании STMicroelectronics.

Как и в случае применения других программных пакетов производства ST, пользователю предлагается использовать их в том виде, в каком они есть. Этим компания снимает с себя ответственность за нецелевое использование программного обеспечения и возможные ошибки, появляющиеся при изменении исходного ПО. Вместе с тем, потребителю позволяется вносить изменения в ПО, использовать его части в своих разработках и передавать третьим лицам на некоммерческой основе. Продажа ПО третьим лицам – запрещена.

Заключение

В настоящее время защита данных при обмене информацией является одной из важнейших задач не только для традиционных сетей, но и для быстрорастущего сегмента Интернета вещей. Компания STMicroelectronics предлагает пользователям микроконтроллеров STM32 бесплатный программный пакет X-CUBE-CRYPTOLIB для создания безопасных приложений. Он включает в себя скомпилированные файлы библиотеки шифрования для различных семейств микроконтроллеров и компиляторов. Кроме того, для пользователей доступны аппаратно независимые и аппаратно зависимые варианты реализации.

Для работы с библиотекой достаточно выбрать подходящий файл и использовать его в своем коде. При этом пакет X-CUBE-CRYPTOLIB также включает массу примеров с использованием API библиотеки шифрования для каждого алгоритма защиты.

Пакет X-CUBE-CRYPTOLIB поставляется бесплатно. Его использование ограничено весьма либеральным лицензионным соглашением.

Литература

1. UM1924. User manual. STM32 crypto library. ST, 2015.
2. ГОСТ Р ИСО 7498-2-99. Взаимовязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации.
3. SLA0048. Software license agreement. ST, 2016.
4. *http://www.st.com/*.

Кристоф Лойодис (STMicroelectronics)

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ST ДЛЯ МАЛОГАБАРИТНЫХ «УМНЫХ» УСТРОЙСТВ

Бесплатное программное обеспечение от компании ***STMicroelectronics*** *сделало* ***микроконтроллеры серии STM8*** *еще привлекательнее для разработчиков* ***малогабаритных «умных» устройств.***

life.augmented

Компания **STMicroelectronics** – мировой лидер по работе с клиентами в сфере применения полупроводниковых приборов. Десятки тысяч разработчиков по всему миру выбирают микроконтроллеры серии STM8 для проектирования «умных» устройств, поддерживающих ритм современной жизни.

Одно из самых значимых событий компании STMicroelectronics на пути совершенствования своей продукции – начало сотрудничества с **Cosmic Software Technology, Inc.** Теперь все инструменты разработки программного обеспечения, которые необходимы инженерам при создании, отладке и настройке оборудования на базе микроконтроллеров серии STM8, доступны без каких-либо ограничений. В то время как другие производители обеспечивают разработчиков инструментарием с узкими функциональными возможностями или лимитированным размером программного кода, современные бесплатные Си-компиляторы для серии **STM8** от Cosmic (COS-C-COMPILER) полноценно поддерживают все исполнения микроконтроллеров семейства STM8, включая устройства с памятью до 128 Кбайт.

Для начала работ по прототипированию устройств с 8-битными микроконтроллерами достаточно приобрести комплект оборудования **STM8S-Discovery,** который обеспечивает основные функции микроконтроллеров семейства **STM8S** (его стоимость составляет всего $8). Помимо STM8S, ориентированного на промышленное применение, серия включает линейку с ультранизким энергопотреблением (**STM8L**) и устройства для применения в автомобильной промышленности (**STM8AF** и **STM8AL**). В целом, семейство STM8 объединяет свыше 120 микроконтроллеров, отличающихся конфигурацией встроенной памяти, корпусным исполнением и периферией: интерфейсами связи, таймерами и конвертерами.

По словам вице-президента, директора сектора микроконтроллеров компании STMicroelectronics *Мишеля Буффа,* семейство STM8 в настоящее время наиболее распространено среди 8-битных микроконтроллеров. Оно занимает значительный объем мирового рынка (около 40% от общего числа проданных микроконтроллеров). Но компания стремится к тому, чтобы микроконтроллеры семейства STM8, благодаря своей простоте и экономичности, находили все большее применение в десятках миллионов реализуемых и проектируемых сегодня устройств.

В свою очередь, менеджер по работе с ключевыми клиентами компании Cosmic Software *Люк Юбиали,* основываясь на продолжительной совместной работе с STMicroelectornics над несколькими поколениями микроконтроллеров серии STM8, считает, что Си-компиллятор CXSTM8 идеально подходит для работы с 8-битной архитектурой этих микроконтроллеров. Он также отмечает, что лучшие в своем классе по производительности и наиболее гибкие в процессе отладки и настройки микроконтроллеры серии STM8 доступны всем потенциальным разработчикам. Более того, в связи с ужесточением требований по безопасности к проектам, компилятор может дополнительно включать узел тестирования и динамической проверки изделия.

Дополнительная техническая информация

Новые бесплатные Си-компиляторы CXSTM8 производства компании Cosmic Software элементарно интегрируются со средой визуальной разработки от STMicroelectronics (*STVD*).

В свою очередь, STVD – это часть общедоступного набора инструментов, который также включает интерфейс визуального программирования (*STVP*), инструмент компоновки программного кода (*ST Assembler Linker*), средства детального анализа и отладки кода (*STMStudio*).

Комплекс STVD включает все необходимые инженеру инструменты для контроля разработки приложения: от создания архитектуры и отладки управляющего кода до программирования микроконтроллера. Также он обеспечивает программно реализованную симуляцию работы и управляет недорогими встроенными отладчиками/программаторами RLink/ST-LINK и передовым эмулятором STice для микроконтроллеров серии STM8.

Си-компилятор долгое время оставался платным программным продуктом, но сейчас разработка устройств на базе микроконтроллеров серии STM8 стала доступнее и удобнее благодаря бесплатному программному обеспечению от компании STMicroelectronics и ее партнеров.

«Получая больше от технологий, получаем больше от жизни», считает руководство компании STMicroelectronics.

В 2015 доходы компании составили $ 6,9 милрд, клиентская база по всему миру превысила 100 000 пользователей.

Литература

1. *http://www.st.com/content/st_com/en/about/media-center/press-item.html/p3802.html.*

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

Вячеслав Гавриков (г. Смоленск)

WI-FI-ПРОЦЕССОРЫ CC3100/CC3200: БЕЗОПАСНОСТЬ ДЛЯ ИНТЕРНЕТА ВЕЩЕЙ

Интернет вещей (IoT) – перспективная технология, которая притягивает не только добросовестных потребителей, но и злоумышленников, использующих лазейки в системах безопасности IoT-устройств для незаконных действий. До сих пор создание по-настоящему защищенных беспроводных IoT-приложений «с нуля» было доступно только для крупных компаний, но на рынке стали появляться бюджетные специализированные решения, например, Wi-Fi-процессоры ***CC3100/CC3200*** *производства компании* ***Texas Instruments.***

В настоящее время Интернет вещей (IoT) объединяет миллиарды устройств и продолжает наращивать популярность. Эта технология чрезвычайно перспективна и весьма привлекательна с финансовой точки зрения. Интерес к ней повышается как со стороны рядовых потребителей, так и со стороны бизнеса в лице крупных и мелких компаний – разработчиков электроники. При таком огромном потенциале и гигантских темпах роста есть все основания полагать, что скоро этот рынок станет интересен и для злоумышленников.

Для многих потребителей Интернет вещей представляется технологией, упрощающей быт: это и своевременный автоматический запуск стиральной машинки, и подогрев воды в бассейне, и прочее. В таком аспекте угроза от хакеров кажется надуманной – вряд ли какой-то злой гений посягнет на то, чтобы подчинить себе все соседские пылесосы. А вот получить доступ к системе охранной сигнализации дома или беспрепятственно проникнуть на склад – угрозы уже более реальные. Однако даже не это главное. Дело в том, что IoT связан с денежными транзакциями, например, Интернет-банкингом, оплатой коммунальных услуг, автоматическими заказами услуг и товаров по Интернету и так далее. Вот здесь и наблюдается основная потенциальная угроза.

Если каналы передачи данных не будут должным образом защищены, то риск остаться без электронных денег значительно повышается. При этом стоит с пониманием относиться к психологии потребителя. Когда он покупает «умную» технику – он вправе рассчитывать на то, что ее производитель уже позаботился о том, чтобы обеспечить должный уровень безопасности. Всегда ли это так? К сожалению не всегда.

Сейчас на рынке IoT соседствуют разработки самого разного уровня: «поделки» от независимых разработчиков IoT, недорогие решения от азиатских малоизвестных или совсем неизвестных производителей, устройства, созданные именитыми компаниями. К сожалению, вероятность того, что первые две из перечисленных групп уделяют достаточно внимания решению проблем безопасности, практически равна нулю.

Главным достоинством устройств от небольших компаний является оригинальность. В Интернете можно отыскать огромное количество самых разнообразных идей. Однако недостаток ресурсов не всегда позволяет доводить до ума даже очень перспективные устройства. Нужны опыт, время и деньги. Если со временем у этой группы производителей и разработчиков все в порядке, то опыта и денег на разработку хватает не всегда.

Малоизвестные азиатские производители редко могут похвастаться высоким уровнем программной безопасности. Для них ключевым фактором часто становится не оригинальность идей и решений, а сверхнизкая цена конечного продукта. К сожалению, стоимость реализации функций и протоколов защиты может оказаться выше, чем разработка и производство самого устройства.

Именитые компании пока не так активны в сфере IoT. Они не спешат вкладывать деньги во все проекты подряд, а только в те, где можно надежно защититься от конкуренции двух вышеперечисленных групп производителей. Устройства ответственных разработчиков очень часто обеспечивают высокий уровень защиты данных, но оказываются достаточно дорогими, а потому доступными не для всех потребителей.

Таким образом, несмотря на то, что стандарты для IoT пока находятся на стадии разработки, уже сейчас можно обозначить минимальный набор требований, которым должны удовлетворять «умные» устройства Интернета вещей, чтоб быть востребованными на рынке:

- обеспечивать высокий уровень безопасности при обмене данными;
- иметь минимальную цену и быть доступными;
- отличаться простотой использования и минимальным энергопотреблением.

Нет сомнений, что все эти задачи можно будет решать быстро и просто, как только появятся специализированные интегральные решения. Ярким доказательством этого становятся новые микросхемы **CC3100/CC3200** для создания Wi-Fi-приложений, производимые компанией **Texas Instruments.**

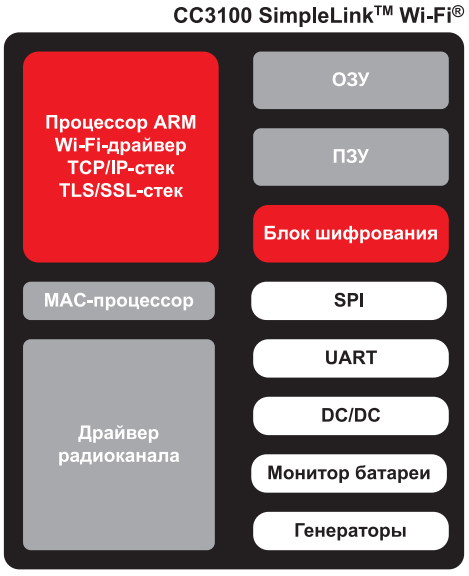


Рис. 1. **Блок-схема сетевого Wi-Fi-сопроцессора CC3100**

Таблица 1. **Сетевые возможности CC3100 [4]**

Область	Категория	Функционал	Примечание
TCP/IP	Сетевой стек	IPv4	Базовый вариант стека IPv4
TCP/IP	Сетевой стек	TCP/UDP	Основные протоколы
TCP/IP	Протоколы	DHCP	Режимы «Клиент» и «Сервер»
TCP/IP	Протоколы	ARP	Поддержка протокола ARP
TCP/IP	Протоколы	DNS/mDNS	Определение адреса по имени (DNS Address resolution) и локальный сервер
TCP/IP	Протоколы	IGMP	До 3 IGMPv3 для управления мультикастом
TCP/IP	Приложения	mDNS	Поддержка мультикастового mDNS для объявления сервисов через IP (service publishing over IP)
TCP/IP	Приложения	mDNS-SD	Протокол обнаружения сервисов через IP в локальной сети
TCP/IP	Приложения	WEB Server/HTTP Server	Формирование статических и динамических ответов с использованием шаблонизатора
TCP/IP	Безопасность	TLS/SSL	TLS v1.2 (client/server)/ SSL v3.0
TCP/IP	Безопасность	TLS/SSL	См. Simple Link Wi-Fi CC3100 SDK для поддерживаемых Cipher Suite
TCP/IP	Сокеты	RAW Sockets	Определяемая пользователем инкапсуляция на уровнях WLAN MAC/PHY или IP
WLAN	Подключение	Policies	Управление подключением и переподключением к той или иной доступной Wi-Fi-сети
WLAN	MAC	Promiscuous Mode	Режим приема всех фреймов с фильтрацией, независимо от того, кому они адресованы
WLAN	Производительность	Initialization time	Менее 50 мс с момента сигнала enable до первого соединения в режиме точки доступа
WLAN	Производительность	Throughput	UDP = 16 Мбит/с
WLAN	Производительность	Throughput	TCP = 13 Мбит/с
WLAN	Инициализация	WPS2	Регистрация нажатием кнопки или с помощью PIN
WLAN	Инициализация	AP Config	Режим точки доступа для первоначального конфигурирования продукта (через WEB-интерфейс и beacon info element)
WLAN	Инициализация	SmartConfig	Альтернативный метод для первоначального конфигурирования продукта
WLAN	Роль	Station	Одиночный клиент (802.11.2bgn) с действующими режимами энергосбережения 802.11
WLAN	Роль	Soft AP	Одиночная точка (802.11.2bgn) доступа с действующими режимами энергосбережения 802.11
WLAN	Роль	P2P	Поддержка P2P в качестве Group Owner
WLAN	Роль	P2P	Поддержка P2P в качестве Client
WLAN	Безопасность	STA-Personal	WPA2 personal security
WLAN	Безопасность	STA-Enterprise	WPA2 enterprise security
WLAN	Безопасность	STA-Enterprise	EAP-TLS
WLAN	Безопасность	STA-Enterprise	EAP-PEAPv0/TLS
WLAN	Безопасность	STA-Enterprise	EAP-PEAPv1/TLS
WLAN	Безопасность	STA-Enterprise	EAP-PEAPv0/MSCHAPv2
WLAN	Безопасность	STA-Enterprise	EAP-PEAPv1/MSCHAPv2
WLAN	Безопасность	STA-Enterprise	EAP-TTLS/EAP-TLS
WLAN	Безопасность	STA-Enterprise	EAP-TTLS/ MSCHAPv2
WLAN	Безопасность	AP-Personal	WPA2 personal security

CC3100 — сетевой Wi-Fi-процессор, позволяющий обеспечить безопасное подключение любого микроконтроллера к сетям Wi-Fi. CC3200 — интегральное решение, объединяющее в одном корпусе функционал сетевого Wi-Fi-процессора и мощь микроконтроллера **ARM Cortex-M4**.

Главными особенностями CC3100/CC3200 являются:

- готовое решение проблем безопасности передачи данных;
- обеспечение максимально быстрого создания Wi-Fi-приложений;
- минимальное потребление;
- минимальная стоимость микросхем;
- наличие готовых средств разработки: программных библиотек, примеров, отладочных наборов и так далее.

Методы организации безопасного обмена в IoT

Интернет вещей напрямую взаимодействует с сервисами электронного банкинга, Интернет-магазинами, сферой услуг, в том числе — и государственных. Все это превращает проблему обеспечения безопасности в одну из ключевых задач отрасли в целом.

С точки зрения злоумышленников каждое IoT-устройство — это потенциальная лазейка к незаконному обогащению. По этой причине крайне важно, чтобы с точки зрения разработчика это же устройство рассматривалось как слабое звено, которое необходимо защищать должным образом. К счастью, сфера безопасности достаточно развита и существуют проверенные методы организации защиты при обмене данными [1]:

- частный обмен с шифрованием (Private communication), при котором данные перед передачей шифруются и могут быть раскодированы только при наличии у принимающей стороны ключа шифрования;
- обмен с аутентификацией пользователя (End-point authentication), когда перед обменом информацией стороны проводят идентификацию друг друга;
- обмен с аутентификацией информации, когда вся критическая и важная информация, например, данные, обновления ПО и прочее, должны иметь цифровую подпись, чтобы подтвердить свой первоисточник.

Перечисленные методы основаны на использовании следующих базовых решений [1]:

- **Шифрование.** Говоря о шифровании, стоит подчеркнуть, что готовые и надежные решения уже созданы. Популярные шифры AES (*Advanced Encryption Standard*), SHA2 (*Secure Hash Algorithm*), RSA и ECC можно считать максимально надежными, так как отсутствуют данные о том, что они были хотя бы раз взломаны.
- **Протоколы безопасности транспортного уровня.** Современная группа протоколов TLS (*Transport Layer Security*) и ее предшественник SSL (*Secure Sockets Layer*) — криптографические протоколы, обеспечивающие защиту данных при обмене между узлами различных сетей. При использовании TSL применяется как шифрование данных, так и метод обмена с аутентификацией конечного узла.
- **Инфраструктура открытых ключей PKI** (*Public key infrastructure*) — основной механизм проведения аутентификации с использованием удостоверяющих центров, которые выступают в качестве доверенного третьего лица при обмене данными между конечными пользователями.

Использование перечисленных методов имеет несколько очевидных преимуществ:

- они уже созданы, и не требуется тратить время на изобретение велосипеда;
- они уже доказали свою надежность и проверены временем;
- они используются во всех современных приложениях от браузеров до социальных сетей, что автоматически решает проблемы совместимости.

Хотя преимущества очевидны, тем не менее, исследования показали, что в сфере IoT описанные методы используют не так часто. Причин для этого много, но стоит выделить наиболее важные из них — чрезмерно высокую сложность программной реализации и высокие затраты по внедрению.

Здесь необходимо сделать небольшое пояснение. Дело в том, что огромное количество IoT-устройств строится на базе маломощных и недорогих микроконтроллеров. Они, с одной стороны, отличаются низкой вычислительной мощностью, а с другой — крайне редко имеют на борту даже элементарные блоки шифрования. В результате такие контроллеры просто физически не могут уместить в себе тяжелые протоколы безопасности TSL/SSL. При этом использование дорогих процессоров со встроенным шифрованием оказывается экономически невыгодным.

Протоколы безопасности TSL/SSL оказываются «не по зубам» не только маломощным контроллерам, но и самим разработчикам. Необходимый опыт имеют единицы, а нанять стороннего программиста небольшому стартапу или скромной компании не под силу.

Возникает странная ситуация, при которой реализация программных методов безопасности оказывается сложнее и дороже, чем создание, производство и написание функционального ПО вместе взятые. Если к этому добавить, что

Рис. 2. **Блок-схема сетевого Wi-Fi-процессора CC3200**

IoT — это, в первую очередь, технология, ориентированная на беспроводную передачу данных, и перед разработчиками стоит задача внедрения Wi-Fi, Bluetooth или аналогичного протокола, то перспективы небольших компаний становятся совсем печальными. Однако не стоит отчаиваться раньше времени: спрос рождает предложение, и на рынке начинают появляться недорогие специализированные устройства, которые снимают с плеч программистов и инженеров-схемотехников груз большинства самых сложных задач. Так, например, новые Wi-Fi-сопроцессоры CC3100 и CC3200 разом решают проблемы безопасности, интеграции в Wi-Fi-сети, уровня потребления и стоимости конечных изделий.

Обзор Wi-Fi-решений CC3100/CC3200 от Texas Instruments

При проектировании сетевых процессоров CC3100/CC3200 компания Texas Instruments стремилась к тому, чтобы максимально упростить жизнь создателям IoT-приложений. Подразумевалось, что CC3100/CC3200 целиком и полностью возьмут на себя вопросы организации Wi-Fi-соединений и решение проблем безопасности при обмене данными, в то время как разработчики сосредоточатся на самом изделии. Рассмотрим особенности каждого из процессоров более подробно.

CC3100 – сетевой Wi-Fi-сопроцессор, позволяющий обеспечить безопасное подключение любого микроконтроллера к Wi-Fi-сетям. В состав CC3100 входят все необходимые для этого блоки (рисунок 1): процессор ARM, выполняющий основные функции (Wi-Fi-драйвер, протоколы Internet), блок коммуникационных интерфейсов для связи с управляющим контроллером, система питания и тактирования.

Wi-Fi-драйвер поддерживает стеки протоколов TCP/IP и TLS/SSL. Он способен выполнять передачу данных на скорости до 13 Мбит TCP и до 16 Мбит UDP (таблица 1) [4]. Допускается одновременная работа до восьми сокетов TCP/UDP и до двух сокетов TLS/SSL [4].

CC3100 может без каких-либо проблем обеспечить подключение практически любого микроконтроллера к сети Wi-Fi. При этом связь между CC3100 и ведущим контроллером организуется посредством UART или SPI. Говоря «практически любой микроконтроллер», имеем в виду, что для реализации TCP-клиента необходимо использовать готовый программный драйвер, который требует 7 кбайт кода во Flash и 700 байт ОЗУ. Впрочем, сейчас это не проблема даже для 8-битных контроллеров.

CC3100 выпускается в компактном корпусе 9x9 мм QFN-64 и работает при температурах -40…85°C. Такого диапазона хватает как для потребительской электроники, так и для промышленных приложений.

Очень важным преимуществом CC3100 является низкий уровень потребления.

CC3200 – сетевой Wi-Fi-процессор, объединяющий в одном корпусе Wi-Fi-модуль и мощный микроконтроллер с ядром ARM Cortex-M4, доступный для программирования пользователем (рисунок 2).

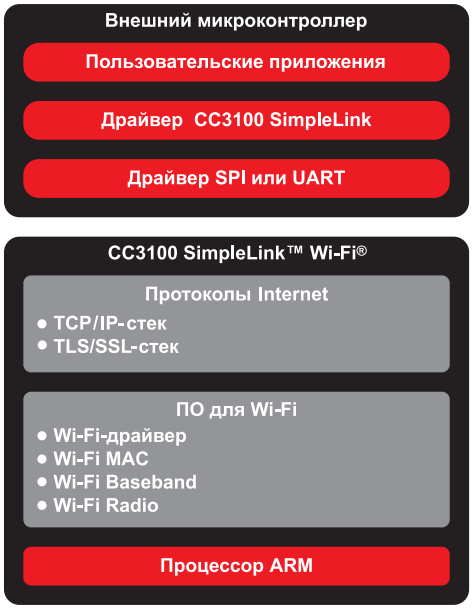


Рис. 3. **Организация ПО при работе с Wi-Fi-процессором CC3100**

Можно заметить, что фактически CC3200 объединяет в своем составе сопроцессор CC3100 и контроллер ARM Cortex-M4. При этом CC3200 выпускается все в том же корпусном исполнении 9x9 мм QFN-64. Таким образом, это решение оказывается идеальным с точки зрения габаритов и простоты создания конечного устройства.

Возможности Wi-Fi-модуля в CC3200 совпадают с возможностями аналогичного блока CC3100, а вот на встроенном процессоре стоит остановиться подробнее. ARM-процессор, интегрированный в CC3200, может похвастать следующими характеристиками:

- ядро ARM Cortex-M4 с рабочей частотой до 80 МГц;
- память: 256 кбайт ОЗУ, SPI для подключения внешней Flash;
- 32 канала прямого доступа к памяти (DMA);
- модули шифрования: AES, DES и 3DES;
- четыре 16-битных таймера с ШИМ;
- 12-битный четырехканальный АЦП;
- последовательный аудиопорт, 1xSD/MMC, 1xSPI, 1xI^2C, 2xUART.

Хотя само ядро является достаточно мощным, но набор периферии по сегодняшним меркам кажется скромным. Тем не менее, с его помощью можно организовать самые разнообразные устройства. Кроме того, ограниченность в данном случае оправдана с точки зрения и стоимости микросхемы, и уровня ее потребления. Так, например, на сайте Texas Instruments заявлена цена CC3100 на уровне $6,7 при заказе от 1000 штук, стоимость CC3200 при покупке партий того же объема составит $8,00. Это сравнимо со стоимостью набора из микроконтроллера и Wi-Fi-модуля, которые не предоставляют функционал TLS/SSL.

Из всего вышесказанного можно сделать вывод о достоинствах CC3100/CC3200. При использовании этих Wi-Fi-процессоров разработчики получают следующие преимущества:

- решение проблем безопасности передачи данных на базе протоколов TLS/SSL;
- максимальное упрощение при разработке Wi-Fi-приложений;
- достижение минимального потребления;
- обеспечение низкой стоимости законченных устройств;
- доступ к готовым средствам разработки, таким как программные библиотеки, примеры, отладочные наборы и так далее.

Вопросы потребления достаточно критичны для IoT-приложений, так как большая часть из них является автономными устройствами. По этой причине следует рассмотреть потребление CC3100/CC3200 более подробно.

Оценка уровня потребления Wi-Fi-устройств на базе CC3100/CC3200

Значительная часть IoT-приложений работает в автономном режиме от аккумуляторов или батареек. Для них уровень потребления – крайне важный параметр. Существует много способов увеличить длительность работы автономных устройств, например, снижать значения питающих токов, использовать различные виды спящих режимов, применять дополнительные альтернативные источники энергии – виброхарвестеры, солнечные батареи и так далее.

При выборе процессора для IoT важно обращать внимание на уровень его потребления и уровень питающих напряжений. Возможность работать с широким диапазоном напряжений позволяет значительно упростить систему питания или даже напрямую работать от батарей без внешних преобразователей.

Сетевые Wi-Fi-процессоры CC3100/CC3200 используют достаточно широкий диапазон напряжений питания, что делает их весьма интересными для совместного использования с традиционными типами батареек и аккумуляторов.

Уровень питающих токов также выглядит достаточно привлекательно. В режиме приема данных по Wi-Fi максимальное потребление CC3100 достигает 53 мА, а в режиме передачи – 223 мА. При этом в режиме ожидания ток падает до 690 мкА, а в состоянии глубокого сна – и вовсе 4 мкА. При этом не стоит забывать о потреблении внешнего управляющего контроллера.

CC3200 при приеме данных по Wi-Fi характеризуется значением тока потребления до 59 мА, а при передаче – до 229 мА. В режиме ожидание ток опускается до уровня 825 мкА. Потребление в состоянии глубокого сна аналогично CC3100 и составляет 4 мА.

Такие показатели, очевидно, располагают к использованию этих процессоров в импульсном режиме. В этом случае большую часть времени они находятся либо в режиме ожидания, либо в режиме сна, пробуждаясь только на время обмена данными по сети Wi-Fi.

При постоянном подключении к сети устройство может находиться в режиме ожидания до 2 с, лишь ненадолго переходя в режим прослушивания сети [2]. При таком алгоритме простое устройство на базе CC3100 сможет работать до года от пары алкалиновых батареек AA.

Рис. 4. **Организация ПО при работе с Wi-Fi-процессором CC3200**

Еще меньше будет потребление, если обмен данными происходит не постоянно, а только по мере необходимости. В таком случае время бодрствования микроконтроллера может составлять от 105 мс, так как именно столько требуется CC3100 для установления безопасного Wi-Fi-подключения.

Особенности написания прикладного ПО для систем на базе CC3100/CC3200

Структура ПО при использовании CC3100 подразумевает использование двух сегментов — пользовательского ПО и программного обеспечения, встроенного в чип CC3100 (рисунок 3).

Нетрудно заметить, что в состав встроенного ПО входят все самые сложные части кода: Интернет- протоколы (TSP/IP и другие), протоколы безопасного соединения (TLS/SSL), протоколы и драйверы для Wi-Fi. Пользователю остается только реализовать функции для работы самого устройства и написать драйвер для работы с CC3100. Впрочем, «написать» — слишком громко сказано, так как в большинстве случаев можно использовать готовые драйверы и примеры и просто интегрировать их в свой код.

Таким образом, при использовании CC3100 программисту потребуется провести инициализацию канала связи (UART и SPI) и правильно применить прикладной интерфейс API, предложенный компанией Texas Instruments. При этом TI стремилась максимально упростить работу с API. В результате оказывается, что для установления защищенного соединения требуется всего десяток строк кода.

Ситуация при использовании CC3200 также оказывается достаточно простой. Структура ПО не меняется (рисунок 4). Единственным, но чрезвычайно важным изменением становится подключение встроенного Wi-Fi-модуля напрямую к матрице Multi-Layer AHB Bus Matrix. Это дает возможность рассматривать данный блок как стандартный периферийный модуль, который способен напрямую взаимодействовать с памятью и ядром, что позволяет достигать максимальных скоростей обмена данных и даже сокращать нагрузку на ядро за счет контроллера прямого доступа к памяти.

В итоге взаимодействие с Wi-Fi-сетью для пользователя максимально упрощается. За «красивой оберткой» прикладного интерфейса API оказываются скрытыми все самые сложные части кода: организация соединений по Wi-Fi и использование протоколов защиты TLS/SSL.

CC3100/CC3200 в своем арсенале имеет широкий набор популярных алгоритмов шифрования, которые используются для механизмов аутентификации и кодирования данных (таблица 2).

Использование API при работе с CC3100/CC3200

Рассмотрим, как выглядит использование API для CC3100/CC3200.

Во-первых, надо настроить защищенное подключение по Wi-Fi. Для этого необходимо наличие трех файлов:

- `/cert/ca.pem` – файл центра сертификации (CA);
- `/cert/client.pem` – файл сертификата открытого ключа;
- `/cert/private.key` – файл закрытого ключа.

Эти файлы используются в инфраструктуре открытых ключей PKI. Для их получения необходимо скачать и установить последнюю версию OpenSSL. Далее в установочной директории `path \bin` запустить `openssl.exe`.

Для получения закрытого ключа используется командная строка: `openssl genrsa -out privkey.pem 2048`, где 2048 — установка разрядности ключа шифрования по умолчанию. Возможно использование разрядности 1024, 2048, 4096 и так далее.

Для получения CA:

```
openssl req -new -x509 -days 3650 -key privkey.pem -out root-ca.pem.
```

Для получения файла сертификата:

```
openssl req -new -key privkey.pem -out cert.pem.
```

Для подписи сертификата необходимо использовать:

```
openssl x509 -req -days 730 -in cert.pem -CA ca.pem -CAkey CAPrivate.pem
set_serial 01 -out cert.pem
```

Более подробное описание процесса создания сертификатов и параметров команд можно найти в руководстве по эксплуатации [3].

Непосредственно для организации соединения существует две функции: `sl_WlanConnect` и `sl_WlanProfileAdd` [3]:

```
sl_WlanConnect(char* pName, int NameLen, unsigned char *pMacAddr, SlSecParams_t* pSecParams, SlSecParamsExt_t* pSecExtParams)
sl_WlanProfileAdd(char* pName, int NameLen, unsigned char *pMacAddr, SlSecParams_t* pSecParams, SlSecParamsExt_t* pSecExtParams, unsigned long Priority, unsigned long Options)
```

В реальном коде использование этих функций потребует от программиста около десятка строк, при этом большая часть из них будет относиться к инициализации используемых структур.

Во-вторых, необходимо инициализировать сокет для защищенного протокола. Это также просто сделать с помощью API. Например, для SSL используется всего одна функция: `sl_Socket(SL_AF_INET, SL_SOCK_STREAM, SL_SEC_SOCKET)`.

В-третьих, для работы с защищенным протоколом используется простой и понятный набор функций: `sl_Close`, `sl_Listen`, `sl_Accept`, `sl_Bind`, `sl_SetSockOpt` и так далее.

В итоге пользовательский код окажется максимально простым и кратким:

```
int CreateConnection(unsigned long DestinationIP)
{
int Status;
SlSockAddrIn_t Addr;
int AddrSize;
```

Таблица 2. **Алгоритмы шифрования, поддерживаемые CC3100/CC3200**

Криптографический алгоритм	Протокол	Назначение	Разрядность ключа шифрования, бит
RC4	WEP, TKIP	Кодирование данных	128
AES	WPA2	Кодирование данных, аутентификация	256
DES	–	Кодирование данных	56
3DES	–	Кодирование данных	56
SHA1	EAP-SSL/TLS	Аутентификация	160
SHA256	EAP-SSL/TLS	Аутентификация	256
MD5	EAP-SSL/TLS	Аутентификация	128
RSA	EAP-SSL/TLS	Аутентификация	2048
DHE	EAP-SSL/TLS	Аутентификация	2048
ECDHE	EAP-SSL/TLS	Аутентификация	160

```
int SockID = 0;
SlTimeval_t timeval;
Addr.sin_family = SL_AF_INET;
Addr.sin_port = sl_Htons(443); // secured connection
Addr.sin_addr.s_addr = sl_Htonl(DestinationIP);
AddrSize = sizeof(SlSockAddrIn_t);
SockID = sl_Socket(SL_AF_INET,
SL_SOCK_STREAM,
SL_SEC_SOCKET);
if( SockID < 0 )
{
// error
while (1);
}
Sl_SetSockOpt(sockID,
SL_SOL_SOCKET,
SL_SO_SECURE_FILES_CA_FILE_NAME,
"rootCA.der",
strlen("rootCA.der"));
Status = sl_Connect(SockID,
( SlSockAddr_t *)&Addr,
AddrSize);
if( Status < 0 && Status != SL_ESECSNOVERIFY )
{
// error
while(1);
}
return SockID;
}
```

Заключение

Технология IoT (Интернет вещей) находится в стадии бурного развития. Сейчас в этой сфере присутствуют самые различные производители и разработчики. Не все из них могут обеспечить надлежащий уровень безопасности при передаче данных. Главной причиной этого является сложность и дороговизна реализации протоколов защиты и методов шифрования.

Компания Texas Instruments предлагает свое решение этих проблем в виде сетевых процессоров CC3100/CC3200. CC3100 – сетевой Wi-Fi-процессор, позволяющий обеспечить безопасное подключение любого микроконтроллера к сетям Wi-Fi. CC3200 – интегральное решение, объединяющее в одном корпусе сетевой Wi-Fi-процессор и мощный микроконтроллер с ядром ARM Cortex-M4.

Благодаря CC3100 и CC3200 даже те разработчики, которые ранее не имели достаточного опыта работы с Wi-Fi и методами защиты данных, смогут создавать надежные IoT-приложения.

Литература

1. Gil Reiter. IoT security made simple with SimpleLink™ Wi-Fi® CC3100 and CC3200 devices. 2016, TI E2E Community.
2. Chris A. Ciufo. TI emphasizes "KISS" in new Wi-Fi ICs. 2014, *http://eecatalog.com/*.
3. CC3100/CC3200 SimpleLink™ Wi-Fi® Interneton-a-Chip User's Guide. 2016, Texas Instruments.
4. Олег Пушкарев. CC3100 – сетевой процессор для «Интернета вещей». Часть I. Новости Электроники, №10, 2014.
5. Олег Пушкарев. CC3100 – сетевой процессор для «Интернета вещей». Часть II. Новости Электроники, №2, 2015.
6. *http://www.ti.com/*.

Хуан Гарсия (Texas Instruments)

СЕНСОРНЫЙ ЗАМОК ОТ TEXAS INSTRUMENTS – ЧАСТЬ СИСТЕМЫ SMART GRID

*Использовав **отладочные наборы Launchpad** и **Touch Boosterpack**, сервопривод, часть деревянного дверного полотна и доработанный врезной дверной замок, инженеры компании **Texas Instruments** продемонстрировали **сенсорный замок,** закрывающийся и открывающийся после набора буквенно-цифрового пароля. В дальнейшем замок можно интегрировать в беспроводную интеллектуальную **систему передачи данных Smart Grid,** разработанную Texas Instruments.*

В данном проекте с помощью отладочных наборов **Launchpad** и **Touch Boosterpack** производства компании **Texas Instruments** был создан сенсорный замок, расширяющий область применения сенсорных технологий и дающий пользователю новый способ ввода и запоминания паролей. В будущем такие устройства позволят заменить традиционные кнопочные клавиатуры, кодовые механизмы и обычные ключи (рисунок 1).

Рис. 1. **Замена традиционных решений сенсорным замком**

Механическая часть устройства включает в себя сервопривод и обычный, но слегка доработанный врезной дверной замок. Чтобы продемонстрировать работоспособность прибора, его смонтировали на небольшом куске дерева, который выполняет функцию дверного полотна (рисунок 2).

Особенности сенсорного замка

Целью проекта было не только продемонстрировать новаторское использование отладочных наборов Launchpad и Touch Boosterpack, но и попытаться оригинально применить вспомогательные материалы, например:

- в качестве корпуса устройства выступает прозрачный кейс для хранения DVD-дисков;
- сенсорный демонстрационный набор Touch Boosterpack закрыт пластиной из прозрачного органического стекла;
- в качестве запирающего механизма используется обыкновенный замок с небольшими доработками;
- станина для сервопривода также разработана с нуля с использованием того же кейса для хранения дисков.

Основными особенностями устройства являются:

- включенный в состав устройства малопотребляющий набор Launchpad;
- включенный в состав устройства сенсорный набор Capacitive Touch Boosterpack, работающий в режиме реального времени;
- прецизионное управление сервоприводом;
- оптимальное управление питанием с помощью системы регуляторов напряжения, расположенных на отладочных платах Launchpad и Touch Boosterpack производства компании Texas Instruments;

Таблица 1. **Расчет срока службы сенсорного замка от четырех батарей 1,5 В 1000 мА·ч**

Среднее время в активном состоянии, с	Срок службы, ч	Число срабатываний	Срок службы, год		
			Входная дверь дома	Школьный шкафчик	Личный шкафчик в спортивном зале
5	22,173	16000	21	9	43
10	22,173	8000	10	5	21
20	22,173	4000	5	2	10

Рис. 2. **Демонстрационный образец сенсорного замка**

• минимальное количество дополнительных компонентов;

• хорошо структурированный код с поддержкой режимов пониженного потребления.

Расчетные значения

Чтобы оценить потенциал этого устройства, необходимо произвести некоторые расчеты. В качестве исходных данных можно взять следующие числовые значения:

• согласно документации, микроконтроллер **MSP430G2452** потребляет максимум 400 мкА при напряжении питания 3 В;

• сервопривод **HiTec 322-HD** потребляет в среднем 180 мА во время активной работы;

• каждая из батарей 1,5 В обеспечивает ток 1000 мА·ч, следовательно, четыре батареи обеспечивают ток 4000 мА·ч.

Используя эти данные, можно произвести оценочный расчет:

• Срок автономной работы от батарей питания определяется в часах с учетом потребления компонентов:

Емкость элемента питания/(потребление сервопривода + потребление процессора) = 4000 мА·ч/(180 мА + 400 мкА) = 22,173 часа.

• Далее необходимо определить среднее число срабатываний замка. Для этого зададимся ориентировочным временем нахождения замка в активном состоянии. Оно определяется скоростью набора кода замка. Будем полагать, что на это уходит порядка 5 с. Тогда, с учетом срока службы аккумулятора в часах, определим ресурс в количествах срабатываний:

Время службы в часах/время в активном состоянии = 22,173/(5 с/3600 с) = 16000 срабатываний!

• Хотя мы получили достаточно большое число, но важно учесть и то, как часто этот замок будет закрываться и открываться. Возьмем, например, входную дверь вашего дома. Если предположить, что вы используете ее дважды в день, то окажется, что ресурса батарей хватит на следующий срок:

Число срабатываний/(число срабатываний в сутки × число дней в году) = 16000/(2 × 365) = 22 года!

В итоге оказывается, что скорее отладочный набор и сами батарейки раньше выйдут из строя от старости, чем сами батарейки разрядятся.

Результаты расчета приведены в таблице 1. Их можно получить самостоятельно, выполняя приведенные вычисления для других условий эксплуатации.

Алгоритм работы

Алгоритм работы устройства представлен на блок-схеме (рисунок 3).

При первом включении необходимо «сбросить» устройство с помощью клавиши “RESET”. Далее ввести пароль длиной 4…30 знаков (касаний), после чего замок закрывается.

Большую часть времени сенсорный замок находится в режиме ожидания и ждет срабатывания датчика приближения. Датчик срабатывает если перед сенсорной панелью провести несколько раз рукой на расстоянии 3…5 см. После этого необходимо ввести пароль. Если он введен правильно — замок закрывается. В противном случае выдается световой сигнал об ошибке ввода.

Руководство пользователя

Алгоритм эксплуатации сенсорного замка достаточно прост:

• если на устройство ранее не было подано питание — включите Touch Boosterpack;

• при первом включении нажмите на клавишу сброса “RESET”;

• введите желаемый пароль;

• нажмите на центральную сенсорную кнопку и проверьте, что отсутствует световая сигнализация об ошибке (пароль должен быть более 4 и менее 30 знаков);

• сенсорный замок закроется;

• через несколько секунд устройство перейдет в спящий режим;

• чтобы его перевести в активное состояние, необходимо несколько раз провести рукой на расстоянии 3…5 см перед сенсорной клавиатурой;

• мигание светодиодов сигнализирует о том, что устройство готово к работе;

• чтобы открыть замок, необходимо ввести пароль и нажать на центральную

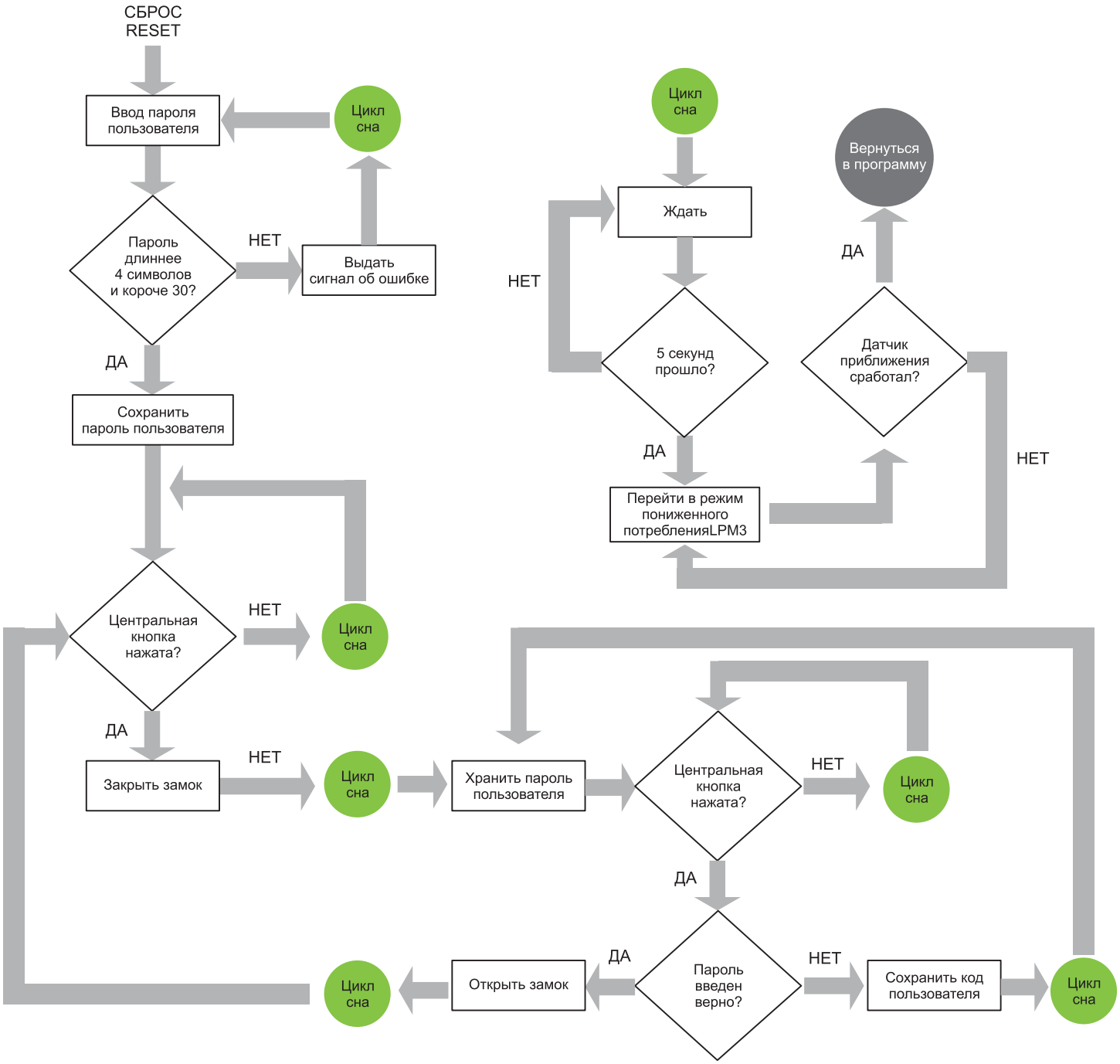


Рис. 3. **Блок-схема алгоритма работы сенсорного замка**

сенсорную кнопку. Проверьте отсутствие мигания светодиода ошибки. Если она возникала – повторите ввод пароля;

- Сенсорный замок откроется.

Дальнейшее развитие проекта

Следующим шагом развития проекта станет интеграция устройства в единую информационную систему. В результате появится возможность не только удаленного управления замком, но и сбор информации о его состоянии. Также предполагается совместная работа в системе Smart Grid производства компании Texas Instruments.

Литература

1. *http://e2e.ti.com/group/launchyourdesign/m/msp430microcontrollerprojects/447755.*

Вячеслав Морозов (г. Ростов-на-Дону)

БЕСПРОВОДНОЙ ИК-ДАТЧИК ДВИЖЕНИЯ: ДЕСЯТЬ ЛЕТ СЛУЖБЫ ОТ ОДНОЙ ЛИТИЕВОЙ БАТАРЕИ

*Системы **автоматического включения освещения,** вентиляции и так далее, реагирующие на присутствие человека – часть автоматизированных систем **«умного дома»** и **«умного производства»,** основанная на **беспроводных инфракрасных датчиках движения.** Стандартный срок непрерывной работы такого датчика от одной литиевой батареи – 4…7 лет. Инженерам компании **Texas Instruments** удалось продлить этот срок до 10 лет, повысив тем самым эффективность системы.*

Беспроводной ИК-датчик движения, реализованный в проекте **TIDA-00489** компании Texas Instruments (TI), демонстрирует возможность непрерывной работы в течение 10 лет от одной литиевой батареи. Этот результат достигнут благодаря использованию в данном проекте наномощных усилителей и компараторов и малопотребляющего микроконтроллера (МК) субгигагерцевого диапазона семейства SimpleLink.

Основные характеристики датчика движения:

- использование наномощных аналоговых микросхем обеспечивает десятилетний срок службы от одной литиевой батареи **CR2032** без ее замены;
- малый ток потребления 1,65 мкА в режиме ожидания (детектор движения при этом находится в активном режиме);
- сверхнизкий ток потребления в активном режиме благодаря применению малопотребляющего микроконтроллера со встроенным радиопередатчиком (1,12 мА в течение 104,1 мс);
- работа в беспроводной сети субгигагерцевого диапазона с управлением по прерываниям;
- работа по прерываниям при передаче центральному контролеру информации о движении объекта обеспечивает экономию электроэнергии;
- дальность обнаружения движения достигает девяти метров.

Области применения:

- автоматизированные системы управления инженерным оборудованием зданий;
- защита от вторжения посторонних лиц;
- обнаружение наличия людей в помещении;
- системы мониторинга помещений;
- системы обнаружения движения;
- устройства с батарейным питанием.

Описание системы

Современные системы промышленной автоматики и автоматизированные системы управления инженерным оборудованием зданий используют датчики движения для управления различными функциями, основанными на присутствии человека, например, освещением, что позволяет повысить эффективность системы, к примеру, выключая освещение, когда в нем нет необходимости. Использование большого числа беспроводных датчиков позволяет сделать системы управления более гибкими для дальнейшего расширения и снизить затраты на установку путем исключения проводных датчиков. Вместе с тем одним из главных ограничений для большой беспроводной сети является организация электропитания, ввиду того, что для систем с питанием от батарей расходы на техническое обслуживание, связанные с периодической заменой этих источников питания, могут оказаться слишком высокими. В зависимости от энергопотребления и конфигурации батарей, пассивные инфракрасные (ИК) датчики движения с батарейным питанием могут работать 4…7 лет без замены батареи.

Разработанный компанией TI малопотребляющий ИК-датчик движения для беспроводной сети субгигагерцевого диапазона увеличивает максимальный срок службы литиевой батареи до 10 лет, благодаря использованию наномощных усилителей и компараторов и беспроводного МК семейства SimpleLink с ультранизким энергопотреблением.

Структурная схема ИК-датчика движения проекта TIDA-00489 показана на рисунке 1. Датчик включает в себя ИК-детектор с аналоговым выходом, два наномощных операционных усилителя (ОУ), два наномощных компаратора, МК беспроводной сети со сверхнизким потреблением и литиевую батарею CR2032. На двух ОУ выполнен активный полосовой фильтр

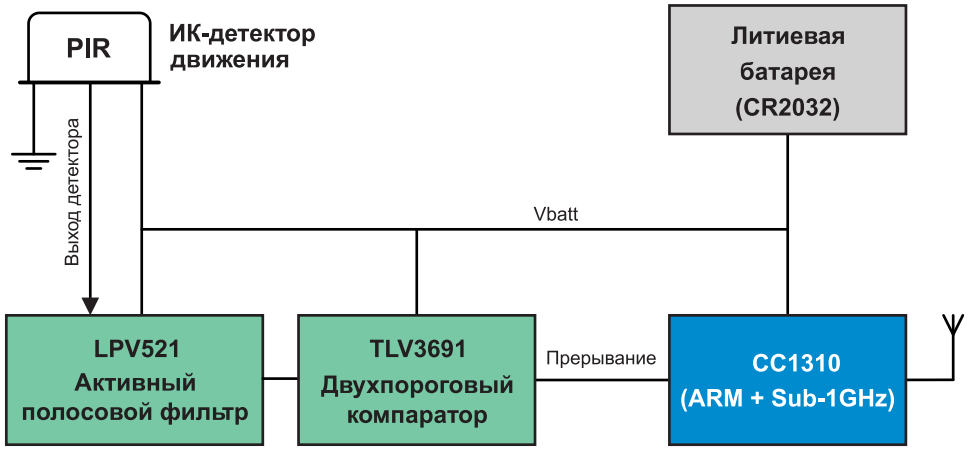


Рис. 1. **Структурная схема беспроводного ИК-датчика движения**

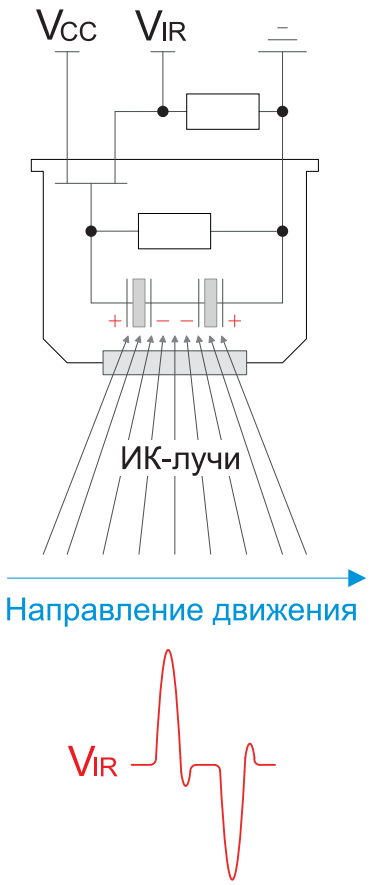


Рис. 2. **Принцип работы ИК-детектора движения**

с высоким входным сопротивлением, что позволяет подключать его непосредственно к выходу датчика, не вносяя нагрузку в его выходную цепь. Два компаратора образуют двухпороговую схему, позволяющую сравнить усиленный выходной сигнал ИК-детектора с фиксированными порогами и отличить полезный сигнал, обусловленный движением объекта, от шума. Два выхода двухпорогового компаратора являются источниками прерываний МК беспроводной сети, благодаря чему МК может оставаться в малопотребляющем спящем режиме до тех пор, пока не будет обнаружено движение, и «просыпаться» только по факту обнаружения движения для отправки сообщения удаленному контроллеру беспроводной сети. Благодаря наноамперному токопотреблению аналоговых компонентов, данный проект TI позволяет достичь десятилетнего срока службы датчика от одной литиевой батареи CR2032.

Принцип работы детектора движения

Использованный в проекте TIDA-00489 маломощный ИК-детектор обнаруживает движение объекта путем выявления в своем поле зрения колебаний энергии ИК-излучения. Поскольку выходной сигнал ИК-детектора имеет очень низкий уровень, его необходимо усилить и отфильтровать от помех, чтобы минимизировать ложные срабатывания датчика движения. Усиленный до необходимого уровня аналоговый сигнал ИК-детектора преобразуется затем в цифровые сигналы посредством двухпорогового компаратора, выходы которого могут быть использованы в качестве источников прерываний МК беспроводной сети, что позволяет активизировать МК только при обнаружении движения.

Пассивный ИК-детектор движения состоит из двух или более пироэлектрических элементов, выходное напряжение которых пропорционально интенсивности падающего на них инфракрасного излучения. Каждая пара пироэлектрических элементов соединена последовательно таким образом, что при воздействии ИК-излучения от окружающей среды в диапазоне комнатных температур и отсутствии движения выходные напряжения каждого элемента одинаковы, и в результате суммарное напряжение на выходе детектора равно нулю. Принцип работы пассивного ИК-детектора движения показан на рисунке 2.

В нижней части рисунка 2 показана форма выходного сигнала детектора при движении объекта с температурой, отличающейся от температуры окружающий среды, параллельно поверхности датчика в поле зрения обоих пироэлектрических элементов. Размах этого сигнала (от пика до пика) пропорционален скорости движения объекта и расстоянию от объекта до детектора, и находится в диапазоне от нескольких милливольт до нескольких сотен микровольт или менее. Полевой транзистор типа JFET используется в качестве повторителя напряжения и обеспечивает постоянное смещение на выходе датчика.

Из-за малых геометрических размеров пироэлектрических элементов для увеличения дальности и поля зрения детектора движения перед ним помещается линза Френеля, которая собирает и фокусирует ИК-излучение на чувствительные элементы детектора движения. Тип линзы обычно выбирается из условий размещения датчика в конкретной окружающей обстановке. Наилучшие результаты применения датчика движения достигаются при движении объекта параллельно поверхности датчика (по сравнению с движением перпендикулярно поверхности датчика), кроме того, датчик следует размещать вдали от сильных источников тепла с меняющейся интенсивно-

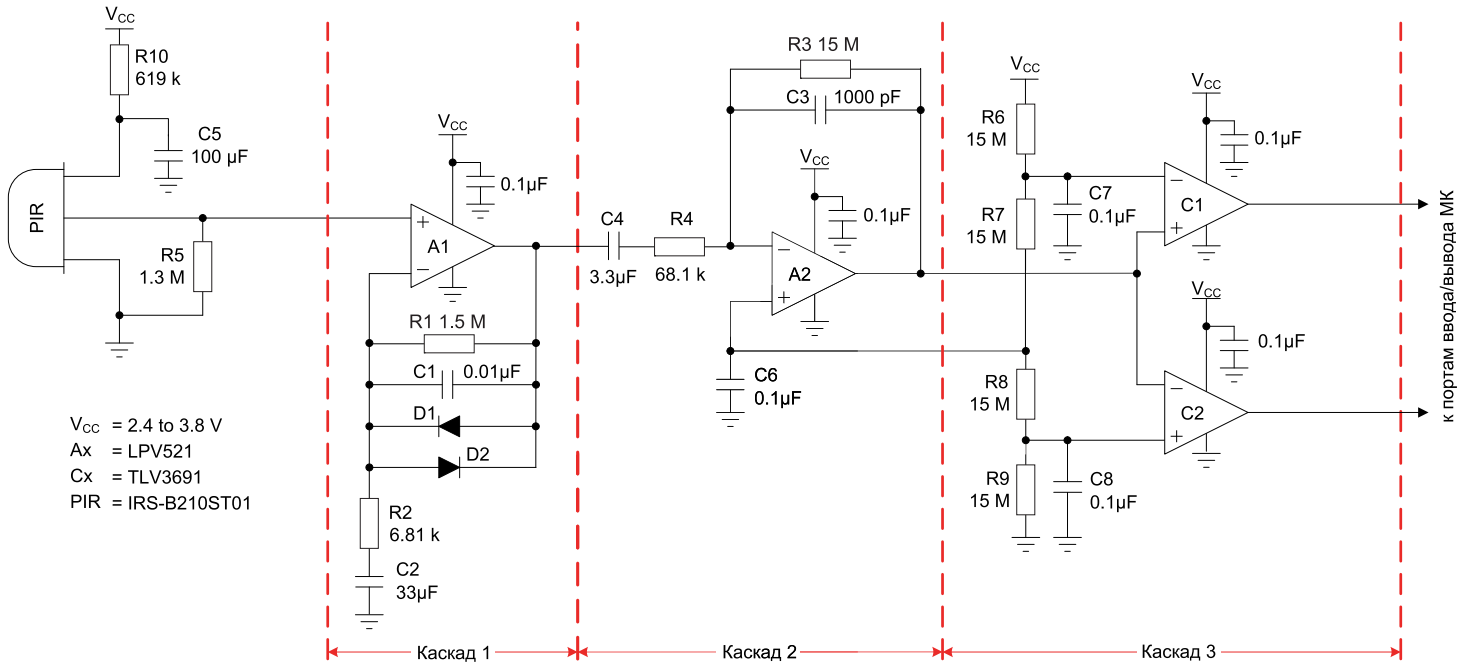


Рис. 3. **Электрическая схема аналоговой части ИК-датчика движения**

стью, например, комнатных вентиляторов и ламп накаливания.

Также следует отметить, что после включения питания необходим интервал времени до 30 с или больше для адаптации пироэлектрических элементов детектора к условиям окружающей среды. Это является ключевым моментом при разработке подсистемы обнаружения движения, так как достижение максимального срока службы батареи предполагает постоянную подачу питания на детектор для обеспечения его правильной работы и надежного обнаружения движения.

Аналоговая часть датчика движения

Электрическая схема аналоговой части датчика движения показана на рисунке 3. Первые два каскада представляют собой активный полосовой фильтр, совмещающий в себе функции усиления и фильтрации сигнала, третий каскад является двухпороговым компаратором. Элементы R_{10} и C_5 выполняют функцию фильтра нижних частот для стабилизации напряжения питания детектора движения. Резистор R_5 задает ток смещения выходного полевого транзистора ИК-детектора движения. Для снижения тока, потребляемого детектором, номинал R_5 выбран больше рекомендуемого значения, при этом из-за уменьшения тока питания детектора происходит снижение его чувствительности и повышение уровня выходного шума, что, однако, является разумным компромиссом для увеличения срока службы батареи. Отчасти потеря чувствительности детектора может быть скомпенсирована увеличением коэффициента усиления и числа каскадов активного фильтра. В связи с более высоким коэффициентом усиления в каскадах фильтра и более высоким уровнем шума на выходе детектора необходимо тщательно оптимизировать расположение высокочастотного полюса фильтра и пороги компаратора, чтобы избежать ложных срабатываний.

Разработка схемы электропитания датчика

Из-за увеличивающегося в течение срока эксплуатации импеданса батареи питания и низкого коэффициента подавления помех по питанию ИК-детектора движения схему питания необходимо спроектировать таким образом, чтобы предотвратить ложные срабатывания в тракте аналогового сигнала от выбросов тока, создаваемых работой МК. Несмотря на то что алгоритм, реализованный в программе МК, помогает фильтровать ложные срабатывания, паразитная петля обратной связи через источник питания может стать серьезной проблемой. В идеале для разрыва паразитной петли обратной связи по питанию ИК-детектор следует питать от стабилизированного источника, однако дополнительный ток покоя стабилизатора приведет к сокращению срока службы батареи, поэтому в данном проекте были исследованы другие способы подавления ложных срабатываний.

На рисунке 4 показана упрощенная схема узла электропитания датчика. Для защиты от подключения батареи в обратной полярности вместо используемого обычно диода Шоттки применен p-канальный МОП-транзистор. Поскольку пиковые токи при работе радиопередатчика находятся в диапазоне 30 мА, использование МОП-транзистора с низким сопротивлением канала R_{DS_ON} обеспечивает значительно меньшее падение напряжения по сравнению с диодом Шоттки. Это позволяет максимально увеличить срок службы батареи, позволяя ей разряжаться до более низкого напряжения, при котором устройство еще может функционировать (более подробно об этом методе читайте в [1]).

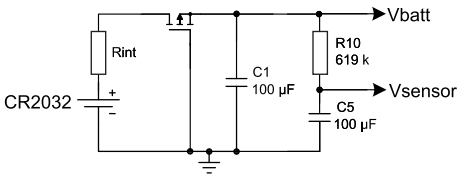


Рис. 4. **Схема электропитания датчика**

Конденсатор C_1 обеспечивает питание схемы в коротких интервалах пикового токопотребления, что позволяет максимально использовать емкость батареи и минимизировать «просадку» напряжения на шине питания, что особенно актуально к концу срока службы батареи, когда значительно увеличивается ее внутреннее сопротивление (обозначенное на рисунке 4 как R_{int}). Де-

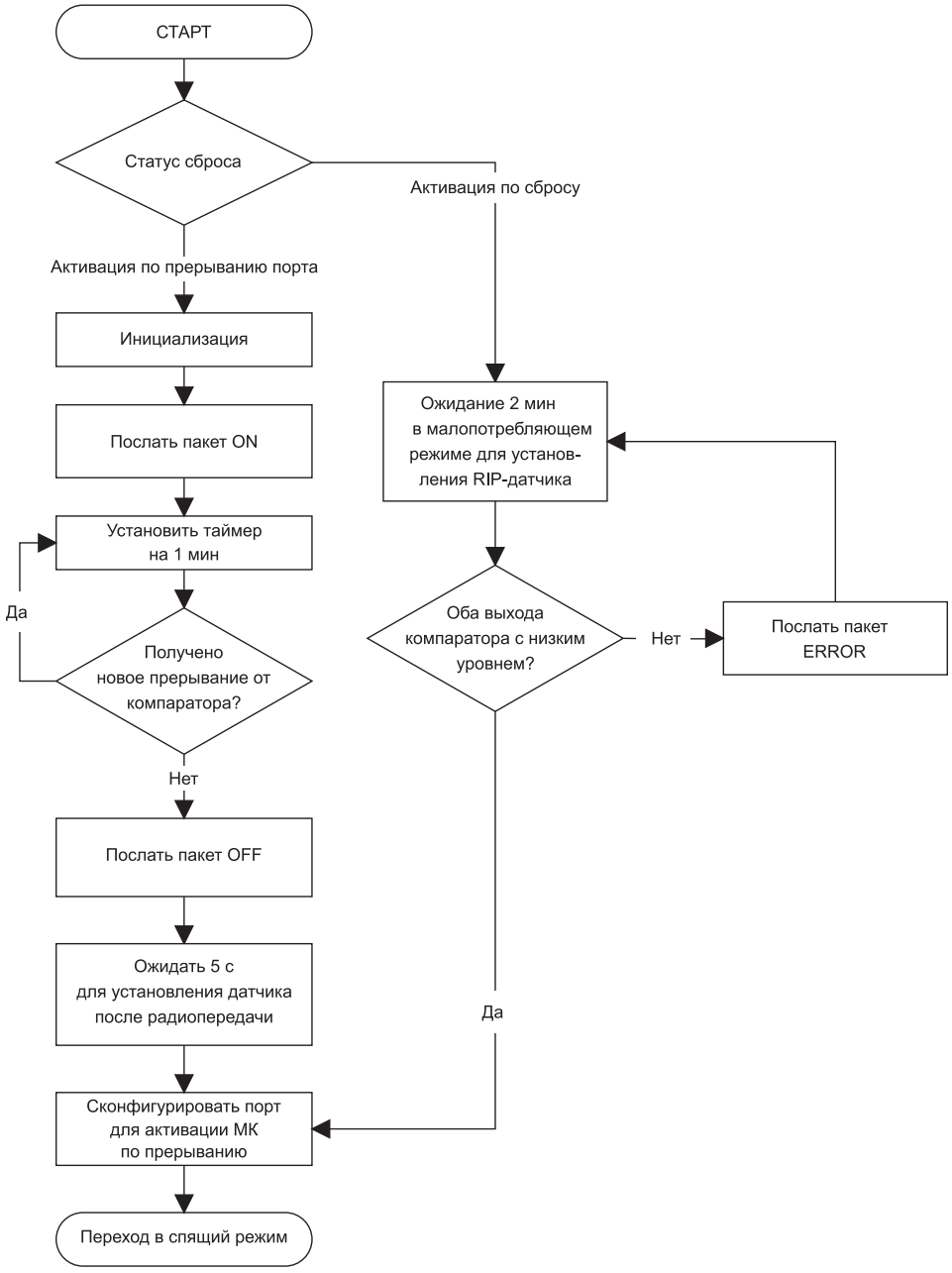


Рис. 5. **Алгоритм работы беспроводного ИК-датчика движения**

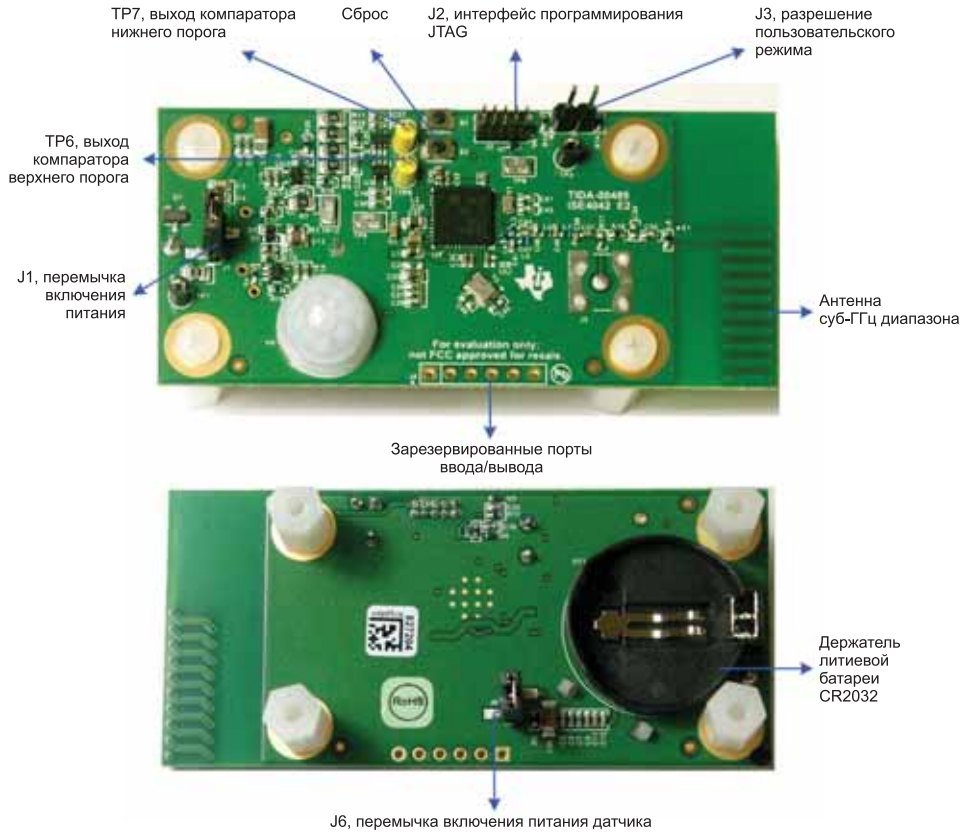


Рис. 6. **Основные элементы макетной платы беспроводного ИК-датчика движения**

тальный расчет необходимой емкости буферного конденсатора C_1 и оценка влияния пиковых токов потребления на срок службы батареи приведены в [2].

Алгоритм работы встроенного ПО

Алгоритм работы беспроводного ИК-детектора движения, показанный на рисунке 5, описывает работу МК **CC1310** в составе макетной платы, разработанной в рамках данного проекта компании TI. Работа программы МК CC1310 начинается с идентификации источника активации. Если пробуждение МК произошло по сигналу сброса, выполняется подпрограмма первого включения — МК CC1310 будет находиться в режиме ожидания в течение двух минут для установления рабочего режима ИК-детектора и аналоговой части схемы. По прошествии двух минут программа проверяет состояние выходов двухпорогового компаратора. В режиме ожидания выходы обоих компараторов должны иметь низкий уровень сигнала. Если какой-либо из выходов компаратора имеет высокий уровень, МК CC1310 посылает сообщение об ошибке (“ERROR”) и снова переходит в режим ожидания до установления рабочего режима датчика. После установления рабочего режима ИК-детектора и аналоговой части схемы МК CC1310 переходит в спящий режим с низким энергопотреблением.

Он будет находиться в спящем режиме до тех пор, пока не получит прерывание с выходов компаратора, означающее, что ИК-детектор обнаружил движение. При пробуждении по прерыванию от ИК-детектора, МК CC1310 посылает пакет “ON”, чтобы сообщить контроллеру сети об обнаружении движения. Далее МК CC1310 будет ожидать неактивного состояния ИК-детектора в течение одной минуты, после чего отправит пакет “OFF” контроллеру сети и вернется в спящий режим.

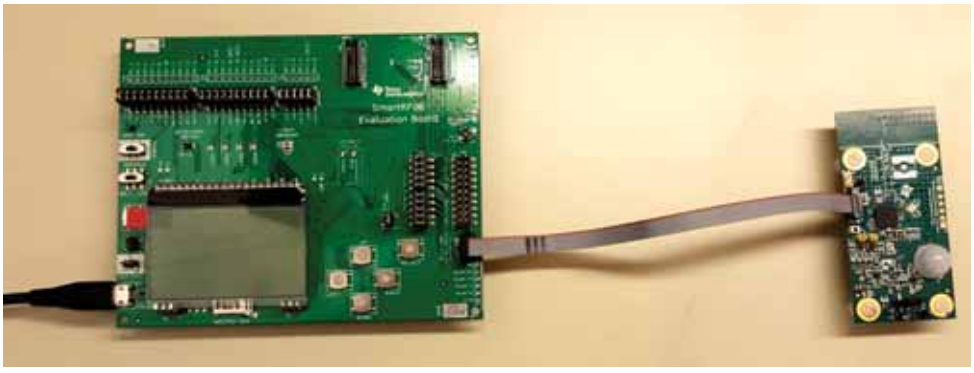


Рис. 7. **Подключение оценочной платы SmartRF06 к макетной плате ИК-датчика движения для программирования и отладки**

Обзор аппаратных средств датчика

На рисунке 6 показан прототип ИК-датчика беспроводной сети субгигагерцевого диапазона с низким энергопотреблением и 10-летним сроком службы литиевой батареи. Печатная плата прямоугольной формы имеет размеры 35x75 мм и поставляется в комплекте с нейлоновыми стойками диаметром 0,5″, упрощающими работу с ней при проведении испытаний в лабораторных условиях.

Все интегральные микросхемы (**CC1310, LPV521** и **TLV3691**), несколько контрольных точек, перемычки и антенна расположены на верхней стороне печатной платы.

На нижней стороне печатной платы размещены держатель литиевой батареи CR2032, перемычка J6 и нижняя часть антенны. Четыре неиспользованных порта ввода-вывода выведены из МК CC1310 на свободную сторону платы, что облегчает в дальнейшем макетирование и отладку устройства.

Конфигурация перемычек

Для облегчения измерения критических параметров и отладки программы в данной макетной плате имеется несколько перемычек, расположение которых показано на рисунке 6. Конфигурация перемычек для рабочего режима выглядит следующим образом: J1 — замкнута, J2 — разомкнута, J3 — разомкнута, J6 — замкнута. Конфигурация перемычек для режима программирования МК CC1310 выглядит следующим образом: J1 — разомкнута (источник питания подключен к выводу 2), J2 — подключена через ленточный кабель к оценочной плате **SmartRF06** (EVM), J3 — разомкнута, J6 — не используется.

Описание контрольных точек макетной платы

Макетная плата ИК-датчика движения включает в себя несколько контрольных точек для измерения параметров сигналов в наиболее важных цепях:

- TP1, TP2 — точки заземления для пробников или общие цепи для измерения напряжения;
- TP6, TP7 — выходы компараторов, соответственно, верхнего и нижнего порогов;
- TP8 — вход встроенного преобразователя постоянного тока в МК CC1310, на который подается отфильтрованное батарейное питание;

• TP9 — отфильтрованное выходное напряжение преобразователя МК CC1310;
• TP13 — выход активного фильтра, являющийся также входом двухпорогового компаратора.

Программные средства датчика

Встроенное программное обеспечение для данной макетной платы было разработано с использованием интегрированной среды разработки (ИСР) Code Composer Studio компании TI (версия 6.1.0). Более подробную информацию по программированию МК CC1310 можно найти в [3].

Для питания платы необходимо напряжение 3,0 В, которое подается на вывод 2 перемычки J1. При использовании внешнего источника питания необходимо учитывать, что подключение питания в этой точке осуществляется в обход схемы защиты от обратной полярности подключения батареи.

Загрузка программного обеспечения

Программирование платы осуществляется путем подключения 10-проводного плоского шлейфа от разъема J2 макетной платы к 10-контактному разъему ARM Cortex Debug Connector P410 оценочной платы SmartRF06 EVM (рисунок 7).

Прием пакетов данных

Как было описано ранее, данная макетная плата TI запрограммирована на обнаружение присутствия человека с помощью ИК-детектора движения. МК CC1310 может передавать значения, соответствующие трем возможным состояниям датчика:

• 0xEE — ошибка при включении датчика (пакет “Error”);
• 0xAA — пакет включения (“ON”) при первом обнаружении движения;
• 0xFF — пакет выключения (“OFF”) через одну минуту после последнего обнаружения движения.

Есть два способа просмотра переданного пакета с целью проверки правильности передачи данных по радиоканалу.

Анализ трафика беспроводных субгигагерцевых сетей автоматизированных систем управления зданиями

Первый способ основан на использовании программы перехвата трафика с графическим интерфейсом пользователя (GUI), работающей на оценочной плате SmartRF06 с радиоканалом, выполненном на **CC13xxEM.** Программа перехвата трафика (*Packet Sniffer Software*) обрабатывает полученный пакет и отображает вычисленные значения на ЖК-экране. Как показано на

Рис. 8. **Работа программы перехвата трафика беспроводных субгигагерцевых сетей автоматизированных систем управления зданиями**

Рис. 9. **Окно запуска программы перехвата трафика**

рисунке 8, программа позволяет отображать только шесть последних принятых значений. Если для тестирования или снятия характеристик системы необходимо большее число данных — следует использовать второй способ, который позволяет регистрировать большее число данных для последующего анализа.

Использование беспроводного USB-адаптера CC1111 и программы SmartRF для перехвата пакетов

Второй способ перехвата трафика основан на использовании беспроводного USB-адаптера **CC1111 USB EVM Kit** 868/915 МГц и программы SmartRF™ Protocol Packet Sniffer. Данные отображаются на экране в исходном виде, однако поток данных может быть подвергнут последующей обработке и использован для тестирования и определения характеристик системы. После установки программы анализа пакетов (версии 2.18.1 на момент написания статьи), процедура обнаружения передаваемых данных выглядит следующим образом:

• Подключите USB-адаптер CC1111 в свободный USB-порт компьютера с установленной программой перехвата трафика.

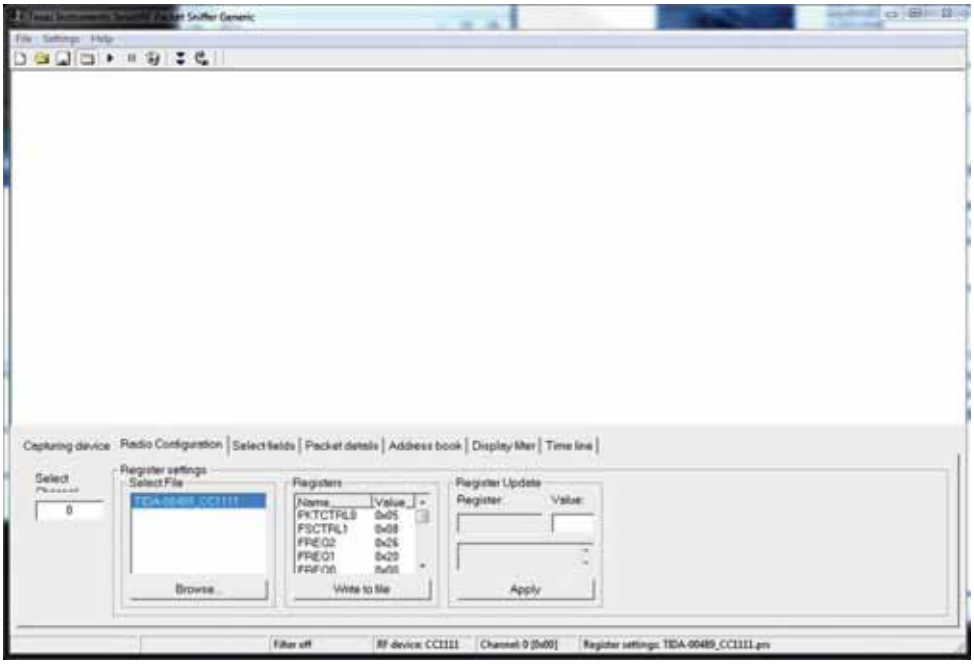


Рис. 10. **Окно настройки конфигурации программы перехвата трафика**

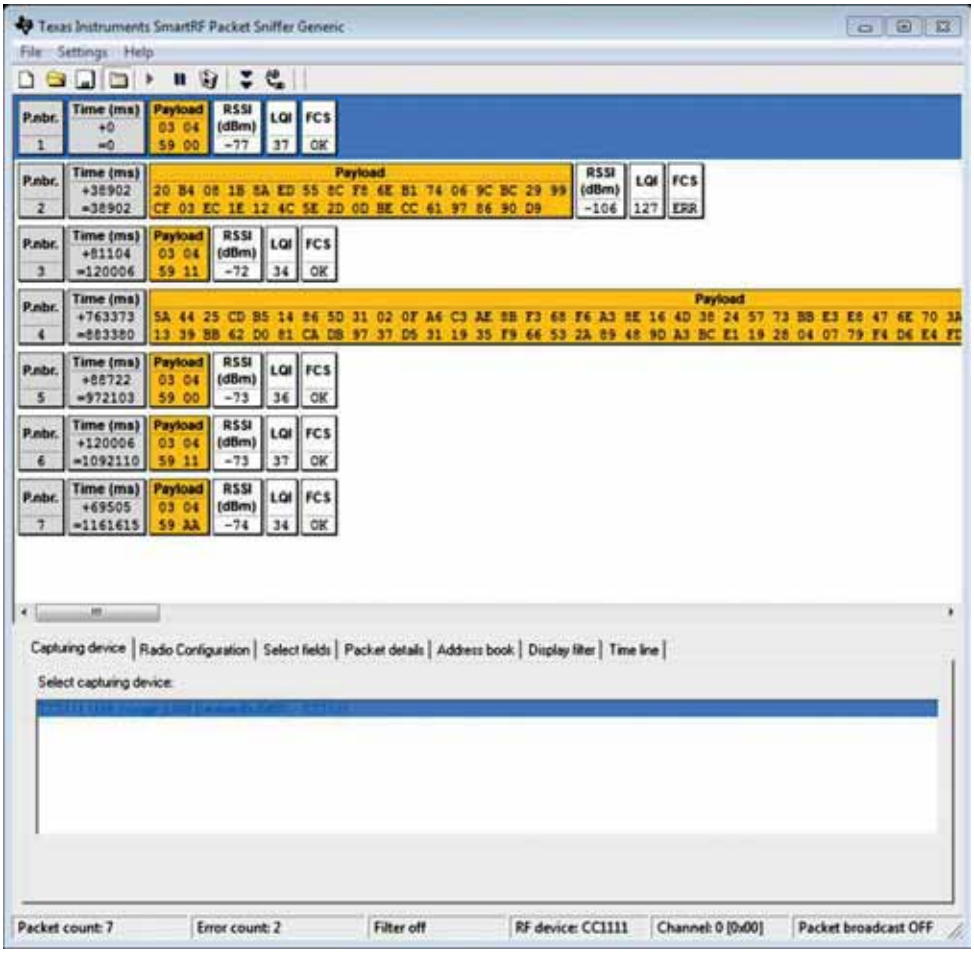


Рис. 11. **Окно неотфильтрованных пакетов данных**

• Запустите программу анализа пакетов, выберите протокол «Generic» и нажмите кнопку “Start” (рисунок 9).

• Настройте CC1111 для корректного отображения пакетов данных. Выберите вкладку “Radio Configuration” (конфигурация радиоканала). Нажмите на кнопку «Browse…», находящуюся под вкладкой “Register settings” (настройки регистров). Откройте файл TIDA-00489_CC1111.prs. Выделите и дважды кликните на «TIDA-00489_CC1111», чтобы применить настройки регистров, показанные на рисунке 10.

• Для запуска процесса перехвата пакетов нажмите кнопку ‘Play” на верхней панели окна программы.

• Программа анализа пакетов может обнаружить посторонние пакеты данных. Примените фильтр для просмотра только достоверных пакетов данных. На рисунке 11 показан пример окна просмотра неотфильтрованных данных. Выделенная строка показывает посторонний пакет данных.

• Для того чтобы добавить фильтр, отображающий только достоверные пакеты, выберите вкладку ”Display filter”. В поле ”Field Name” из выпадающего списка выберите «FCS». Нажмите на кнопку «First». Измените настройки фильтра так, чтобы показывать только пакеты с отметкой «OK», введя «FCS = OK» в поле ”Filter condition», далее нажмите кнопку ”Add”, а затем – кнопку «Apply». На рисунке 12 показаны примеры окна просмотра отфильтрованных данных.

• Для экспорта перехваченных отфильтрованных пакетов нажмите на кнопку “Save the current session” (“сохранить текущий сеанс”) на панели инструментов (значок с изображением дискеты) или приостановите перехват пакетов и нажмите File → Save data… из контекстного меню файла. В в обоих случаях программа предложит сохранить отображаемые данные как пакет данных перехвата (файл с расширением .psd).

• Используйте программу редактора шестнадцатеричных чисел, например, HexEdit, для отображения данных из файла .psd в удобочитаемом виде.

• Откройте файл .psd в программе “HexEdit”, нажмите Tools → Options. В окне “Options” программы “HexEdit” нажмите Document → Display и измените значение “Columns” («Столбцы») на «2066». Нажмите Edit → Select All и Edit → Copy As Hex Text. Откройте текстовый редактор (например, «Блокнот»), вставьте шестнадцатеричные числа в виде текста и сохраните текстовый файл. Этот текстовый файл можно импортировать в электронную таблицу программы Microsoft® Excel® для дальнейшего анализа. Для получения дополнительной информации о формате перехваченного пакета данных нажмите Help → User Manual.

Характеристики энергопотребления

Ток потребления различных функциональных узлов датчика был измерен на предварительном макете. Эта информация использовалась в процессе разработки для того чтобы найти разумный компромисс между сроком службы батареи с одной стороны и характеристикой чувствительности детектора движения и напряжением питания

датчика — с другой. Эти же данные были использованы для сравнения с результатами испытаний окончательного варианта макета, чтобы убедиться в хорошей корреляции между предварительными и окончательными результатами. Кроме того, на прототипе была исследована зависимость потребляемого тока от напряжения питания. Результаты измерения тока потребления приведены в таблицах 1 и 2.

Как видно из данных, приведенных в таблице 1, существует хорошая корреляция между измеренными в макетной плате значениями тока потребления и номинальными расчетными значениями. Данные из таблицы 2 показывают также небольшую положительную зависимость потребляемого тока от напряжения питания. Это означает, что расчет срока службы батареи на основе средних значений тока потребления выполнен с запасом ввиду того, что потребляемый ток будет уменьшаться по мере старения батареи.

Два основных режима работы, показанные в таблице 2, соответствуют режимам, описанным на рисунке 5. В столбце «Разность токов» показано, насколько увеличивается потребляемый ток при переходе из спящего в активный режим — это значение используется при расчете срока службы батареи. Последняя строка в таблице 2 добавлена исключительно в ознакомительных целях, так как при таком низком напряжении питания значительно увеличивается выходной шум ИК-детектора движения, вследствие чего возрастает вероятность ложных срабатываний датчика. Ток потребления при минимальном напряжении питания был измерен с помощью пользовательской программы, удерживающей МК в спящем режиме и игнорирующей прерывания, вследствие чего в таблице 2 нет данных по току потребления в активном режиме при этом напряжении питания.

Данные по энергопотреблению были использованы в следующем разделе для расчета планируемого срока службы батареи в различных условиях эксплуатации.

Расчет срока службы батареи

Расчет времени автономной работы макетной платы осложняется наличием множества различных вариантов применения и условий эксплуатации данного типа датчиков. Подход к решению этой задачи основан на вычислении среднего значения для двух вероятных, но отличающихся друг от друга условий эксплуатации и одного наихудшего варианта использования датчика. Эти условия использования датчика представлены следующим образом:

- вариант 1 (наихудший) — 10 движений в час каждый час в течение всего срока службы батареи. Каждое движение объекта в поле зрения датчика является

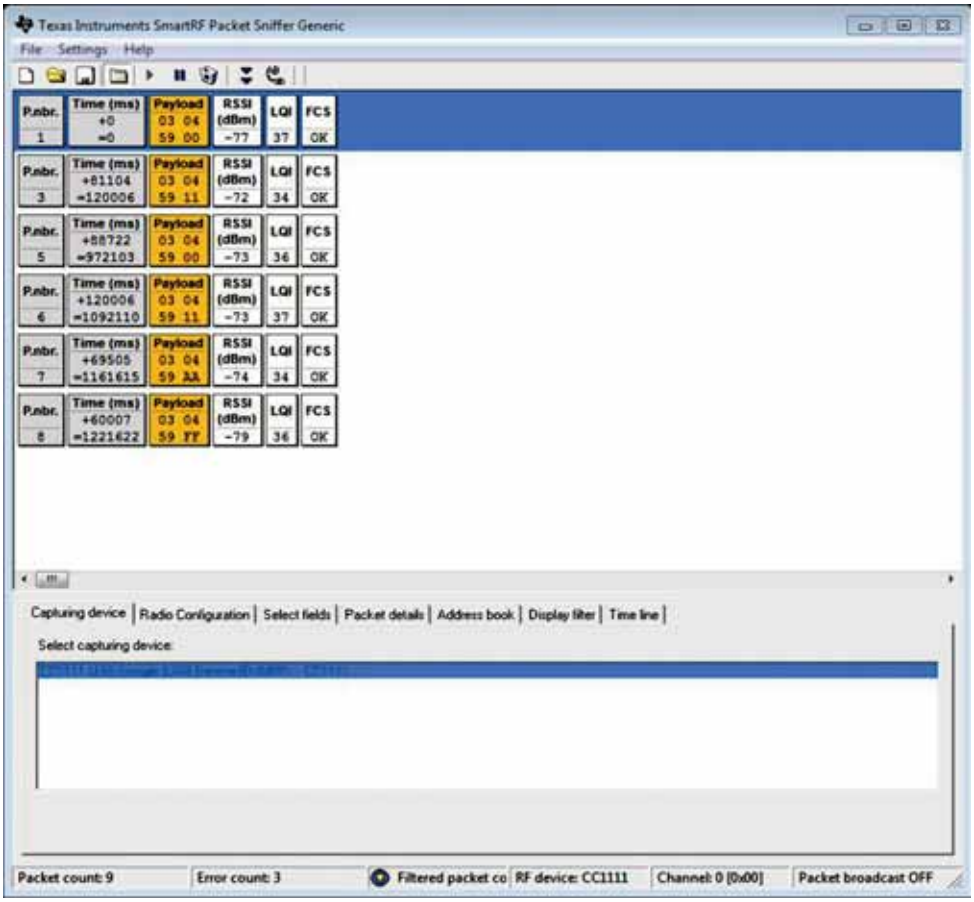


Рис. 12. **Окно отфильтрованных пакетов данных**

Таблица 1. **Ток потребления различных функциональных узлов датчика**

Функциональный узел датчика	Ток потребления в спящем режиме, нА	
	Номинальное значение	Измеренное значение
Детектор движения	600	594
Сдвоенный компаратор	150	150
Делитель	50	50
Операционный усилитель 1	374	360
Операционный усилитель 2	409	380
МК CC1310	100	120
Всего для датчика	1683	1654

Таблица 2. **Ток потребления датчика в различных режимах работы**

Напряжение питания Vcc, В	Ток потребления, мкА		
	Спящий режим	Активный режим	Разность токов
3,8	1,75	2,46	0,71
3,6	1,73	2,45	0,72
3,3	1,69	2,36	0,67
3,0	1,65	2,3	0,65
2,7	1,64	2,28	0,64
2,4	1,6	2,22	0,62
2,2	1,59	–	–

Таблица 3. **Чувствительность ИК-детекторов движения в различных режимах работы**

Наименование	Ток потребления в спящем режиме, нА	Vout, В DC	Максимальная дальность обнаружения при Av = 90 дБ, м	Максимальная дальность обнаружения при Av = 70 дБ, м
R_S = 2,2 МОм, R_D = 1 МОм				
IRS-B210ST01	365	0,78	6,1	1,83
IRS-B340ST02	355	0,764	7,62	2,44
IRA-E700ST0	500	1,093	3,66	1,37
IRA-E712ST3	555	1,204	3,96	1,52
R_S = 1,3 МОм, R_D = 620 кОм				
IRS-B210ST01	594	0,77	> 9,14	1,98
IRS-B340ST02	572	0,744	8,23	2,44
IRA-E700ST0	838	1,085	4,57	1,52
IRA-E712ST3	920	1,178	5,18	2,29

отдельным событием, то есть вызывает прерывание и, по завершении работы таймера, МК возвращается в спящий режим до появления следующего прерывания.

• вариант 2 — офисное помещение, 14 часов спящего режима и 10 часов непрерывного движения, при котором таймер не успевает сброситься до следующей активации.

• вариант 3 — помещение с непостоянным характером движения в рабочее время, 14 часов спящего режима и 10 движений каждый час в течение 10 часов, причем каждое движение, как и в случае 1, является отдельным событием.

Одним из способов оптимизации срока службы батареи в данной макетной плате является продолжительность активного режима таймера. Значение по умолчанию в программе составляет одну минуту. Поскольку этот параметр можно легко изменить, для демонстрации возможности увеличения срока службы батареи случаи 1 и 3 были пересчитаны для продолжительности работы таймера 30 с.

Формула для расчета срока службы батареи выглядит следующим образом:

$$\text{Срок службы (лет)} = \frac{\text{Емкость батареи} \times 1 \times \text{Понижающий коэффициент}}{(\text{Ток спящего режима} + \text{Добавочный ток}) \times 8760\ \text{ч/год}},$$

где

Добавочный ток = [(Разность токов × Отн. длит. актив. режима) – (Ток передат. × Отн. длит.)] × Число событий.

Понижающий коэффициент в формуле учитывает саморазряд батареи. Анализ результатов расчетов показывает, что планируемый средний срок службы батареи в данной макетной плате с установкой таймера на 1 минуту составляет 11,22 года. Пересчет срока службы для случаев 1 и 3 с установкой таймера на 30 с дает значения, соответственно, 9,9 и 11,99 года. Средний срок службы батареи с установкой таймера на 30 с составляет таким образом 11,34 года. Для наихудшего случая установка таймера на 17 с или менее увеличивает срок службы батареи как минимум до 10 лет.

Функциональные характеристики

Чувствительность детектора движения

Чувствительность датчика была измерена для нескольких типов детекторов движения с различными параметрами цепей питания и двух коэффициентов усиления Av активного фильтра. В таблице 3 приведены сводные данные результатов этих измерений. Выделенная ячейка этой таблицы показывает чувствительность детектора движения для конфигурации, реализованной в макетной плате данного проекта TI.

Дальность беспроводной связи

Дальность передачи данных по радиоканалу, измеренная в типичной офисной обстановке с частичным перекрытием линии прямой видимости, составила 220 м. Уровень радиосигнала на максимальном удалении, измеренный с помощью анализатора пакетов CC1111, составил менее – 100 дБм?. Несмотря на то, что полученную дальность, учитывая малые размеры антенны на печатной плате, можно считать отличным результатом, имеются способы увеличения этого расстояния. Первый из них основан на использовании штыревой антенны, имеющей более высокий коэффициент усиления по сравнению с антенной на печатной плате. Другим способом является увеличение мощности передатчика CC1310 до максимального уровня за счет некоторого увеличения потребляемого тока в моменты передачи данных.

Литература

1. Application Report: Reverse Current/Battery Protection Circuits, *http://www.ti.com/lit/an/slva139/slva139.pdf*.

2. White Paper SWRA349: Coin cells and peak current draw, *http://www.ti.com/lit/wp/swra349/swra349.pdf*.

3. Быстрый старт разработки беспроводного канала 868 МГц на CC1310. Новости Электроники №3, 2016 г.

Виктор Чистяков (г. Малоярославец)

ДЛЯ УМНЫХ СИСТЕМ С АВТОНОМНЫМ ПИТАНИЕМ: БЕСПРОВОДНОЙ ДЕТЕКТОР CO

*Аналоговые компоненты с **энергопотреблением на уровне наноампер** и сверхэкономичная **микроконтроллерная платформа TI SimpleLink** – именно эти изделия производства Texas Instruments позволили компании разработать **беспроводной детектор окиси углерода** со сверхнизким энергопотреблением и возможностью работы от одной батареи типа CR2032 до 10 лет.*

Во многих системах промышленного оборудования и автоматизации зданий используются датчики окиси углерода (CO), чтобы предупредить о достижении опасного уровня концентрации этого газа. Все чаще в таких системах устанавливают беспроводные контрольные датчики, чтобы снизить затраты на монтаж оборудования и обеспечить удобное расширение системы за счет устранения проводов.

Новый прибор производства компании **Texas Instruments** (TI) включает наномощные операционные усилители и компараторы, системный таймер, датчик температуры и микроконтроллерную мультистандартную беспроводную платформу для диапазона 2,4 ГГц (рисунок 1). Современные компоненты позволили создать детектор окиси углерода со сверхнизким энергопотреблением и чрезвычайно длительным временем автономной работы.

Обзор системы

Компактное устройство работает в составе беспроводной сети и обеспечивает удаленный и полностью автоматизированный сбор показаний с контролем заданного уровня концентрации окиси углерода, известного также под названием угарный газ. Предусмотрена периодическая автоматическая проверка исправности устройства.

Особенности детектора CO:

- чрезвычайно малое потребление электроэнергии обеспечивает 10-летний срок службы миниатюрной батареи **CR2032** или аналогичной;
- датчик окиси углерода и аналоговые цепи постоянно включены, чтобы обеспечить постоянный контроль и быстрое время отклика;
- беспроводная технология Bluetooth Low Energy (BLE) снижает затраты на установку и позволяет нескольким удаленным датчикам работать с одним центральным узлом (хостом);
- предусмотрена периодическая самопроверка и контроль разряда батареи с отправкой отчетов о состоянии каждые пять минут (конфигурируемый параметр);
- контроль концентрации CO в диапазоне 0…1000 частей на миллион (ppm) с точностью ±15%.

Основные области применения детектора CO:

- системы пожарной безопасности: обнаружение углекислого газа;
- системы вентиляции и кондиционирования: детекторы качества воздуха и наличия газа;
- автоматизация зданий.

Состав детектора

Микросхемы и датчики, применяемые компанией Texas Instruments в составе беспроводного детектора, позволяют максимально увеличить срок службы элементов питания.

Основными компонентами устройства являются наномощные операционный усилитель, компаратор и таймер, а также МК со сверхнизким энергопотреблением и поддержкой BLE. В составе платы детектора есть также датчик температуры и электрохимический датчик CO (рисунок 2). На базе ОУ реализован трансимпедансный усилитель (ТИОУ) для усиления и фильтрации тока от электрохимического датчика CO. Когда выходное напряжение ТИОУ достигает соответствующего опасной концентрации уровня CO, компаратор генерирует прерывание для беспроводного МК. Таким образом микроконтроллер может работать с минимальным потреблением энергии все время, пока уровень CO находится в допустимых пределах, и просыпается только для того, чтобы контролировать уровень CO, когда он достигает опасных пределов. Наномощный таймер системы генерирует периодические прерывания для беспроводно-

Рис. 1. **Беспроводной детектор концентрации CO**

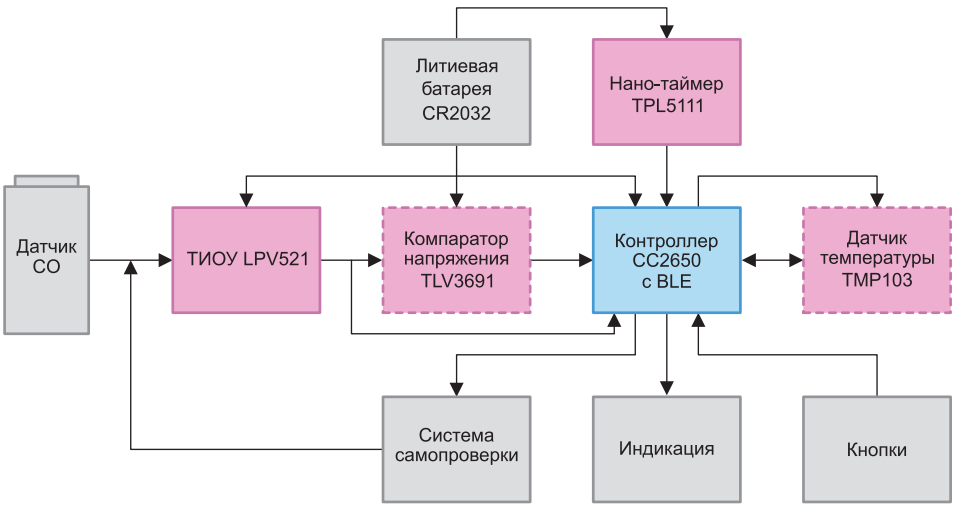


Рис. 2. **Блок-схема детектора концентрации CO**

го МК таким образом, чтобы МК мог проверять датчик и отправлять сигнал статуса системы на центральный узел. Датчик температуры используется для коррекции показаний концентрации CO в зависимости от температуры окружающей среды. Энергопотребление в цепях аналоговых компонентов на уровне наноампер и ультранизкое потребление беспроводного МК обеспечивают 10-летний срок автономной работы от одной батареи типа CR2032.

Операционный усилитель

Составляющий лишь несколько наноампер выходной ток электрохимического датчика газа поступает на вход ОУ, где должен быть преобразован в напряжение и усилен с помощью ТИОУ. Функция фильтрации позволяет ограничить шум, попадающий на вход компаратора и АЦП МК, а также обеспечивает необходимую задержку при скачкообразных изменениях концентрации газа.

Идеальным для этой конструкции является ОУ **LPV521** с низким током и напряжением входного смещения, что позволяет использовать на входе высокоомные резисторы, а также сигналы с полным размахом напряжения как на входе, так и на выходе. Потребляемый LPV521 ток составляет всего 351 нА (типичное значение), что способствует чрезвычайно длительному сроку службы батареи. Кроме того, LPV521 включает защиту от электромагнитных помех, чтобы уменьшить чувствительность детектора к паразитным сигналам ВЧ, что полезно для микропотребляющих устройств из-за наличия каскадов с высоким импедансом.

Компаратор

Для максимальной экономии электроэнергии МК большую часть времени находится в выключенном состоянии и активизируется только когда концентрация CO достигает опасного уровня. Для этого схема компаратора преобразует усиленный и отфильтрованный выходной сигнал датчика в цифровой сигнал, который может быть использован в качестве пробуждающего прерывания для МК.

Низкое потребление тока, всего 75 нА (типичное значение), а также низкие напряжение и ток смещения по входу делают **TLV3691** идеальным выбором для данной задачи. Входной каскад TLV3691 работает с синфазными сигналами, амплитуда которых может на 100 мВ превышать полный размах напряжения. Тем самым предотвращается инверсия по фазе сигнала на выходе, когда напряжение входного сигнала превышает напряжение питания. Это не только ставит заслон шуму источников питания, но также расширяет возможности по установке порога компаратора в этом устройстве.

Микромощный беспроводной микроконтроллер

Получаемую от датчика информацию необходимо передавать в центральный узел обработки. При этом, как и в любом изделии с батарейным питанием, система радиопередачи и процессор должны обладать пониженным энергопотреблением. Важным фактором при разработке устройства является требуемый для оконечного оборудования протокол беспроводной связи.

Процессоры на базе беспроводной платформы TI SimpleLink включают радиомодуль и обладают сверхнизким энергопотреблением, что позволяет обеспечить для удаленных датчиков чрезвычайно длительный срок работы от батареи. Кроме того, **CC2650** является многопрофильным стандартным устройством с поддержкой программного обеспечения для Bluetooth Smart, ZigBee, 6LoWPAN и ZigBee RF4CE. В этом детекторе TI использован протокол Bluetooth Low Energy, но аппаратное оборудование может также работать и с другими протоколами.

Наномощный системный таймер

С помощью наномощного таймера **TPL5111** этот детектор CO способен

Таблица 1. **Основные характеристики беспроводного детектора CO**

Параметр	Значение
Датчик газа	Figaro TGS5342 (электрохимический)
Антенна Bluetooth	Антенна на печатной плате
Источник питания	Литиевая батарея CR2032 (3,0 В)
Взаимодействие в сети	По умолчанию рассылка пакетов BLE каждые 5 минут
Визуальная индикация	Два светодиода для индикации режимов работы и превышения концентрации газа
Калибровка	Чувствительность датчика газа и усиление трансимпедансного ОУ с программированием через интерфейс UART
Средний ток в дежурном режиме, мкА	1,07
Расчетное время автономной работы, лет	>10
Диапазон беспроводной связи, м	>54
Условия эксплуатации	Температура 50°C при влажности 40% ± 10% Температура 0°C при влажности 30% ± 5%
Диапазон концентрации газа, ppm	0…1000
Размеры, мм	43,18x104,14

чрезвычайно долго работать от одной батареи питания. TPL5111 заменяет внутренний таймер любого стандартного МК. Дискретно-аналоговый системный таймер потребляет гораздо меньше энергии, чем внутренний таймер МК. Таймер может быть использован как для того чтобы вывести МК из режима сна подачей запроса прерывания, так и для того чтобы полностью отключить питание системы – в целом или частично.

Временной интервал таймера устанавливается пользователем с помощью резисторов и может составлять от 100 мс до двух часов с типовой точностью 1%. TPL5111 регулярно выводит МК из режима сна, чтобы он мог выполнять ряд задач, включая контроль датчика и передачу служебных сигналов в центральный узел.

Датчик CO

В качестве электрохимического датчика CO использована двухвыводная модель **Figaro TGS5342.** Этот датчик был выбран на основании рабочих характеристик в различных условиях окружающей среды и при разных уровнях концентрации CO. Датчик отличается низким энергопотреблением, что способствует обеспечению 10-летнего срока службы без замены батареи.

Можно предполагать, что результаты, полученные после испытаний с этим датчиком, могут быть достигнуты и с иными двухполюсными электрохимическими датчиками со схожими характеристиками.

Датчик температуры

Выходной ток датчика CO может зависеть от температуры. Например, при концентрации 400 ppm ток на выходе датчика TGS5342 может быть на 20% выше при 60°C и почти на 40% ниже при 0°C по сравнению с выходным током при 20°C.

CC2650 вычисляет концентрацию газа с использованием внутренней таблицы коррекции температур для показаний, считываемых с **TMP103.** Разрешающая способность TMP103 составляет 1°C. Таблица температурной коррекции была взята из технического описания датчика. Для экономии электроэнергии и продления срока службы батареи напряжение питания подается на датчик TMP103 только при чтении показаний температуры.

Элемент питания

Источником питания этого детектора является литий-ионный элемент CR2032 в форм-факторе «монета». Выбор CR2032 был обусловлен повсеместной распространенностью этого типа батарей, особенно для таких компактных систем, как удаленные датчики.

CR2032 имеет идеальные рабочие параметры по напряжению. Напряжение элемента остается относительно стабильным на протяжении почти всего цикла разряда практически до полного истощения запасов энергии. После чего выходное напряжение падает относительно быстро.

Также при низких температурах у литий-ионных батарей стабильнее температурные характеристики, чем у щелочных элементов. Это преимущество связано с использованием в литий-ионных элементах неводного электролита, который работает лучше, чем водные, обычно используемые в щелочных батареях. Тем не менее, батарея CR2032 и газовый датчик ограничивают температурный диапазон всего устройства. Использованные интегральные схемы и другие электрические компоненты пригодны для работы в более широком диапазоне температур, чем батарея и газовый датчик. Таким образом, указанный диапазон рабочих температур детектора CO составляет 0…50°C.

Последовательно с батареей в схеме установлен p-канальный МОП-транзистор с низким сопротивлением канала, а параллельно – сглаживающий конденсатор. Имея минимальное прямое падение напряжения в нормальном режиме работы, p-канальный МОП-транзистор предотвращает повреждение компонентов схемы, если батарейка вставлена в обратной полярности. Сглаживающий конденсатор позволяет предотвратить провалы напряжения, особенно во время сеансов беспроводной связи.

Требования к батарее

Устанавливайте только литиевую батарею **Energizer CR2032VP** или аналогичную, которая имеет:

- напряжение: 3,0 В;
- минимальную емкость: 240 мА·ч;
- разрядный ток: 0,19 мА.

Описание работы системы

Детектор CO измеряет концентрацию окиси углерода методом контроля выходного тока электрохимического датчика CO. Поскольку выходной ток очень мал, он должен быть преобразован в сигнал напряжения, усиливаемый до приемлемого уровня и в то же время фильтруемый, чтобы удалить шум и свести к минимуму ложные срабатывания. Усиленный аналоговый выходной сигнал преобразуется в цифровой вид с помощью компаратора, выход которого может быть использован как прерывание для пробуждения МК, находящегося большую часть времени в спящем режиме. Сигнал с аналогового выхода может быть также непосредственно оцифрован внутренним АЦП беспроводного МК. Программное обеспечение может через простую формулу преобразовать значения выборок из сигнала в эквивалентную концентрацию окиси углерода.

Основные характеристики детектора CO, разработанного компанией TI, представлены в таблице 1.

Принцип действия газового датчика

Принцип действия датчика основан на явлении протекания специфичной химической реакции (электрохимической реакции) в электрохимической ячейке, представляющей собой емкость с раствором электролита с рабочим (анод) и измерительным (катод) электродами.

Анализируемый газ (в данном случае угарный газ CO) вступает в химическую реакцию с электролитом, заполняющим ячейку (см. рисунок 3). В результате в электролите возникают заряженные ионы, между электродами начинает протекать электрический ток, пропорциональный концентрации анализируемого компонента в пробе. Так как существует линейная зависимость между током и концентрацией газа, датчик может быть откалиброван с использованием газа известной концентрации. Другие значения концентрации могут быть получены на основе уровня выходного сигнала датчика.

Базовая трансимпедансная схема для усиления и фильтрации выходного тока датчика газа показана на рисунке 4. Когда газовый датчик подвергается воздействию CO, электрический ток протекает от рабочего к измерительному электроду. ТИОУ преобразует ток датчика в напряжение с коэффициентом усиления, устанавливаемым резистором обратной связи RF. Комбинация RF и CF определяет верхнюю границу фильтра НЧ. Производители датчиков CO иногда рекомендуют устанавливать резистор RL, чтобы добавить стабильности этой цепи, когда сопротивление слишком мало. Рекомендуемое значение RL берется из технического описания датчика CO.

Выходной ток электрохимических датчиков может изменяться в зависимости от температуры окружающей среды. В случаях, когда требуется повышенная точность в широком диапазоне рабочих температур, можно отрегулировать показания датчика с использова-

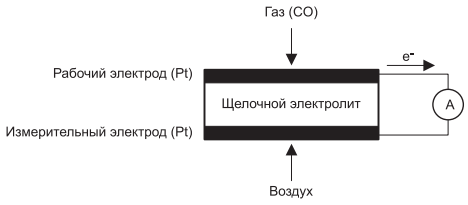


Рис. 3. **Принцип действия электрохимического датчика газа**

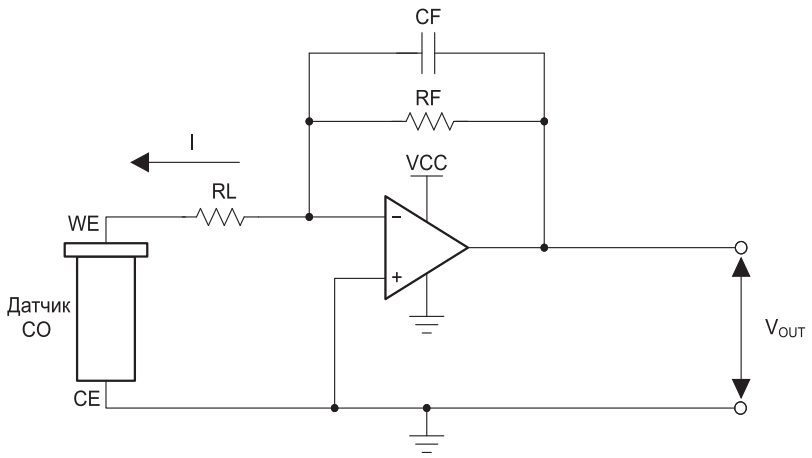


Рис. 4. **Базовая схема трансимпедансного усилителя для газового датчика**

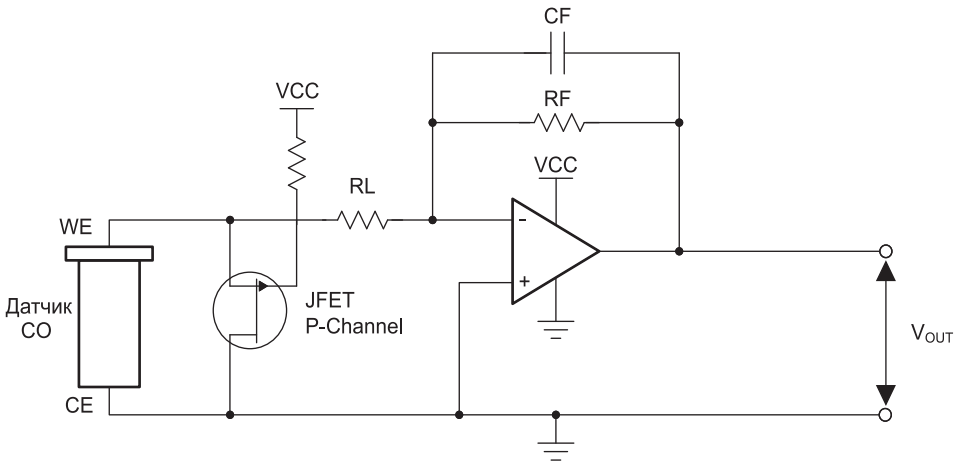


Рис. 5. **Антиполяризационная схема датчика с использованием p-канального транзистора**

нием таблицы коррекции температуры в программном обеспечении. Данные о влиянии температуры на показания датчика могут быть получены из технического описания датчика.

Поляризация датчика

Датчик поляризуется после длительного хранения при отсутствии связи между рабочим и измерительным электродами. Поляризованный датчик может потребовать несколько минут или часов для стабилизации показаний после подключения к рабочей цепи.

Чтобы предотвратить поляризацию датчика при отключении питания от системы, необходимо закоротить выводы датчика или установить между ними сопротивление менее 1 кОм. Есть несколько способов для достижения этой цели. Как показано на рисунке 5, в данном детекторе CO используется полевой транзистор JFET с подключенным к датчику p-каналом, а затвор транзистора подключен к шине питания системы VCC. При выключении питания канал JFET открывается, создавая короткое замыкание между рабочим и вспомогательным электродом. При подаче напряжения питания на устройство канал JFET закрывается, и ток от датчика поступает на вход ТИОУ.

При выборе МОП-транзистора JFET с p-каналом необходимо тщательно учитывать напряжение отсечки $V_{GS(off)}$, чтобы JFET не включался во время обычной работы. Напряжение $V_{GS(off)}$ для JFET должно быть больше, чем минимальное рабочее напряжение. Чтобы предотвратить поляризацию датчика, в этом детекторе CO используется транзистор **MMBFJ270** производства компании **Fairchild.** Максимальное $V_{GS(off)}$ в 2 В обеспечивает закрытый канал, даже когда батарея начинает терять емкость.

Самопроверка датчика

Рабочее состояние газового датчика должно постоянно контролироваться таким образом, чтобы любые сбои могли быть выявлены с передачей сообщения на центральный узел. В этом детекторе CO реализована модифицированная версия схемы самопроверки, описанной Figaro в технической документации к датчику TGS5342.

Функция самопроверки включает пропускание через датчик небольшого тока (примерно 1 мкА) в течение короткого промежутка времени (примерно 4…5 с), в то время как датчик отключен от ТИОУ. Затем, после отключения тестового тока, проводится мониторинг датчика. Анализируя реакцию датчика на испытательный ток, МК может определить его рабочее состояние, а также такие проблемы как короткое замыкание, обрыв цепи и потерю чувствительности.

В этом детекторе, разработанном компанией TI, функция самодиагностики запускается через один из выводов МК (рисунок 7). Чтобы начать испытание, МК устанавливает на этом выводе высокий логический уровень. Это приводит к тому, что p-канальный транзистор JFET Q2 закрывается, тем самым отсоединив датчик от ТИОУ. При этом с выхода МК испытательный ток поступает непосредственно на датчик через резистор R5. Для прекращения подачи испытательного тока МК устанавливает на выводе низкий логический уровень, и в этот момент JFET открывает канал, снова подключая датчик к TIA.

В цепи самопроверки здесь использован транзистор MMBFJ270, который имеет максимальное напряжение отсечки 2 В, чего достаточно для работы схемы даже при логическом уровне на управляющем выводе МК в 2,68 В.

Величина R5 была выбрана, исходя из необходимости обеспечить через датчик ток около 1 мкА, что предполагает на выводе МК минимальный высокий уровень 2,68 В.

На рисунке 6 показана нормальная реакция датчика после протекания испытательного тока в течение пяти секунд. МК в течение секунды контролирует выходное напряжение ТИОУ после отключения испытательного тока. Датчик и схема ТИОУ считаются рабочими, если выходное напряжение (канал 2) более 2,3 В.

В случае обрыва в цепи датчика контролируемое напряжение окажется равным нулю. Если в цепи датчика будет короткое замыкание, то на выходе вместо контрольного импульса будет зарегистрирован небольшой постоянный уровень напряжения и до, и после подачи тестового импульса на датчик.

На основании считанных в процессе тестирования уровней напряжения ПО способно сделать вывод о работоспособности датчика. По завершении тестирования датчику требуется время на восстановление. Чем больше длительность тестового токового импульса, тем больше времени потребуется для восстановления датчика. В прошивке детектора заложен 30-секундный интервал для восстановления датчика после тестирования.

Частые проверки датчика приводят к повышенному расходу энергии батареи. В оригинальном ПО детектора тестирование выполняется каждые 5 минут.

Аналоговые цепи

Аналоговые цепи детектора показаны на рисунке 7. Выходной ток датчика газа поступает на вход ТИОУ с низкочастотным фильтром. Расположенный вслед за ТИОУ компаратор предназначен для генерации прерывания к МК, когда достигнута определенная концентрация газа. Транзистор Q1 используется для предотвращения поляризации датчика, а Q2 используется МК для проверки датчика.

ТИОУ

Есть ряд вариантов для построения принципиальной схемы каскада ТИОУ. Выбор, в конечном счете, зависит от требований к производительности системы в целом. В данном случае не требуется высокая пропускная способность из-за медленной реакции датчика на изменение концентрации газов. Это позволяет использовать ОУ с узкой полосой пропускания. Еще одним ключевым аспектом в этом случае является низкое входное напряжение смещения на операционном усилителе для предотвращения смещения напряжения за счет внутреннего сопротивления датчика СО.

Каскад ТИОУ усиливает выходной сигнал датчика и реализует низкочастотный фильтр. Усиление ТИОУ, равное $1{,}78 \cdot 10^6$ В/А, было выбрано для получения максимального значения выходного сигнала в требуемом диапазоне концентраций газа (0…1000 ppm) при условии сохранения диапазона допустимых входных напряжений для АЦП МК. Выбранная частота среза фильтра нижних частот составляет 0,89 Гц. Частота среза зависит от шума в системе и требуемого времени реакции на изменение концентрации газа. Формулы 1 и 2 позволяют вычислить усиление (A_{TIA}) и частоту среза (f_{high}) для каскада ТИОУ.

$$A_{TIA} = \frac{V_{OUT}}{I_S} = RF1 = 1{,}78 \cdot 10^6\ (\text{В/А}) \qquad (1)$$

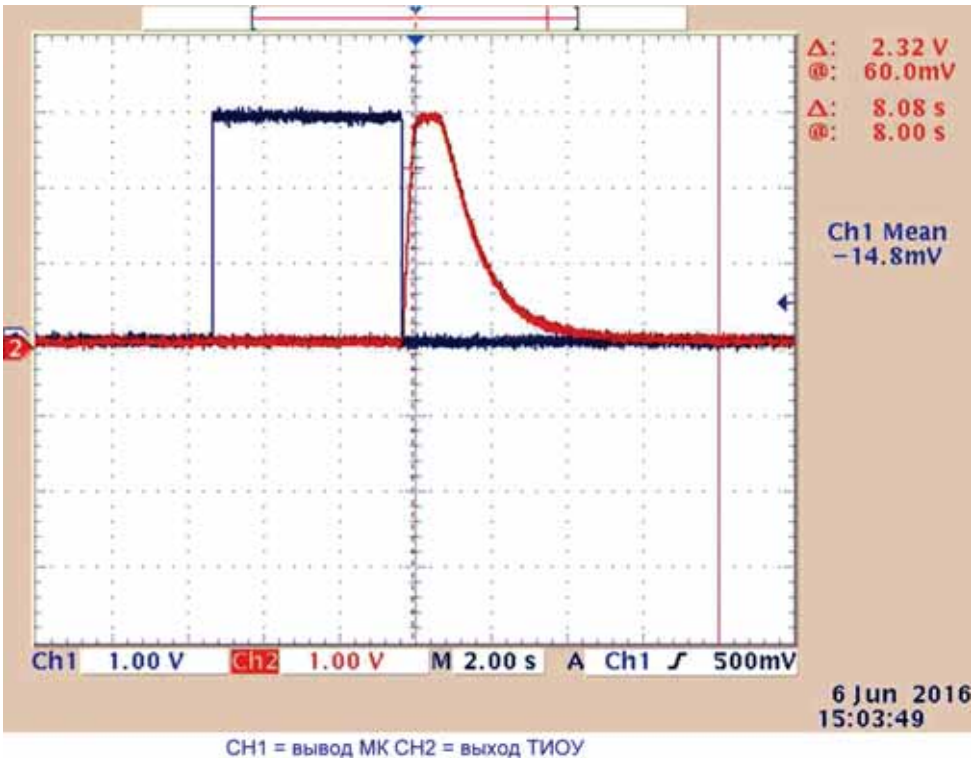
$$f_{high} = \frac{1}{2\pi \times RF1 \times CF1} = 0{,}89\ \text{Гц} \qquad (2)$$

В формуле 1: V_{OUT} — выходное напряжение U1, а Is — ток датчика.

$$V_{OUT} = C_{GAS} \times Sensitivity \times TempCorr \times A_{TIA} \qquad (3)$$

По формуле 3 рассчитывают значение V_{OUT}. При максимальной чувствительности 1,4 нА/ppm для выбранного датчика TGS5342 выходное напряжение V_{OUT} для ТИОУ будет приблизительно 2,49 В при температуре 20°С. При температуре 60°С выходной ток датчика увеличивается примерно в 1,15 раза, следовательно, V_{OUT} возрастет приблизительно до 2,87 В.

В формуле 3 Cgas — заданная концентрация газа (ppm), Sensitivity — чувствительность газового датчика (выраженная в нА/ppm), TempCorr — поправочный температурный коэффициент (взятый из техпаспорта датчика), A_{TIA} — усиление трансимпедансного усилителя (выраженное в В/А).



CH1 = вывод МК CH2 = выход ТИОУ

Рис. 6. **Нормальная реакция датчика на тестовый ток**

Компаратор

Показанная на рисунке 7 схема компаратора преобразует аналоговый выходной сигнал ТИОУ в цифровой сигнал, который используется в качестве прерывания для МК, когда концентрация СО достигает заданного уровня.

Делители на резисторах R4 и R6 устанавливают порог, определяющий уровень СО, при котором формируется прерывание для МК. Конденсатор C8 необходим для стабилизации порогового напряжения, чтобы предотвратить дребезг сигнала на выходе компаратора.

Этот конденсатор имеет небольшую емкость из-за использования высокоомных резисторов в делителе, но он должен иметь низкий ESR (эквивалентное последовательное сопротивление) и низкую утечку. Предпочтительно использовать керамический конденсатор.

В конструкции детектора используется отличающийся незначительным потребляемым током компаратор **TLV3691.** Вход TLV3691 поддерживает входной синфазный сигнал с превышением на 100 мВ уровня напряжения питания. Это не требуется для детектора, но позволяет максимально расширить диапазон регулировки порога компаратора.

На выходе компаратора будет высокий уровень сигнала, когда уровень СО находится ниже порогового значения. Когда уровень СО достигает порогового значения, выход компаратора переключается на низкий уровень.

Порог срабатывания компаратора устанавливается путем регулировки делителем напряжения R4 и R6.

В данном случае потенциометр R6 позволяет легко изменять пороговое значение.

Источник питания

Из-за растущего в течение срока эксплуатации импеданса батареи и низкого подавления помех по цепи питания датчика СО нужно спроектировать систему питания так, чтобы предотвращать выбросы тока, генерируемые МК и приводящие к ложным срабатываниям через канал аналогового сигнала. При том, что реализованный в прошивке алгоритм помогает фильтровать подобные помехи, эта нежелательная обратная связь через источник питания может вызывать проблемы.

В идеале питание датчика должно регулироваться так, чтобы устранить эту обратную связь. Тем не менее, в такой схеме дополнительно потребляемый регулятором ток сократит срок службы батареи, поэтому были рассмотрены другие методы. На рисунке 8 показана упрощенная схема системы электропитания. Вместо традиционного диода Шоттки здесь используется МОП-транзистор для защиты от переполюсовки батареи.

Поскольку пиковые токи находятся в диапазоне 10 мА, когда работает радиопередатчик, использование МОП-транзистора с малым R_{DS_ON} обеспечи-

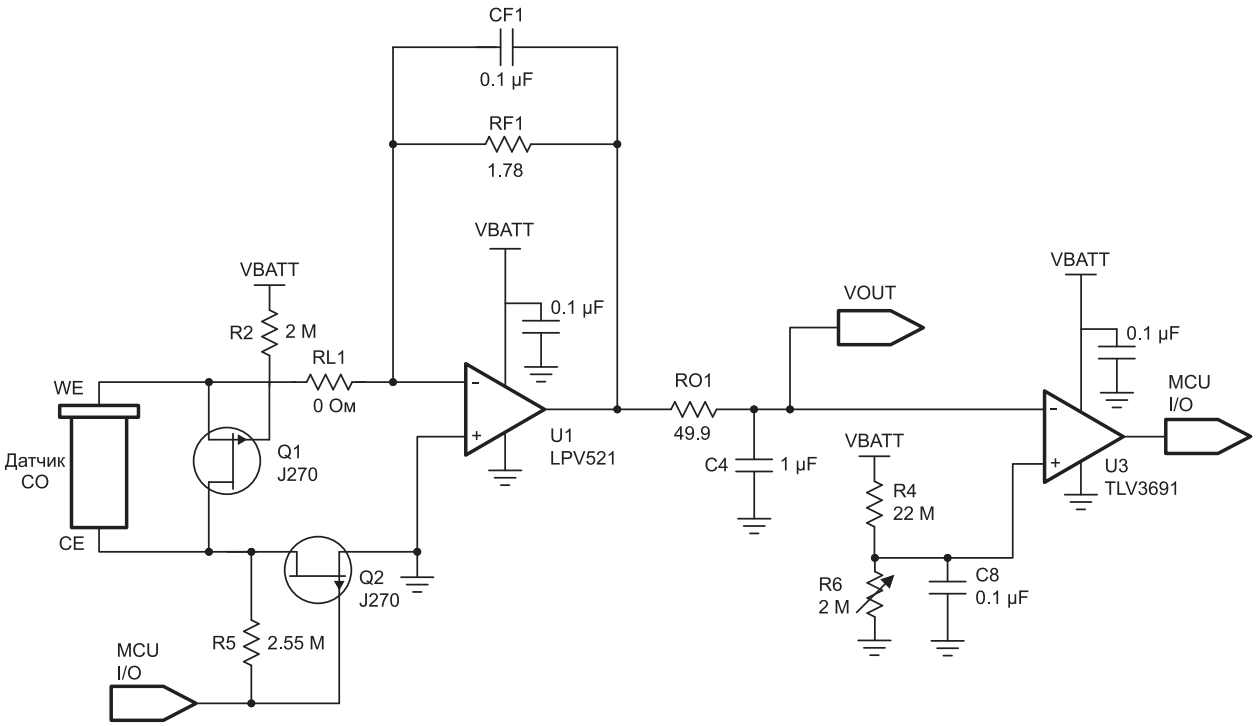


Рис. 7. **Аналоговые цепи газового детектора**

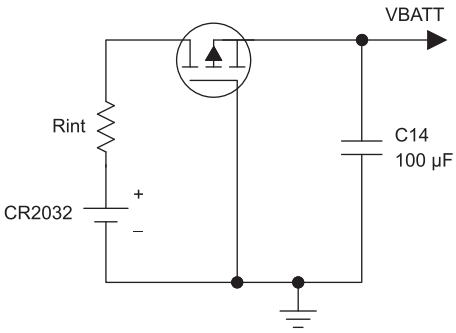


Рис. 8. **Упрощенная схема источника питания для детектора газа**

вает значительно более низкое падение напряжения на нем по сравнению с диодом Шоттки. Это помогает максимально продлить срок службы батареи, позволяя ей разряжаться до более низкого напряжения, прежде чем схема не сможет далее функционировать.

Конденсатор C14 подпитывает схему в периоды высокого и пикового энергопотребления, что позволяет максимально увеличить емкость батареи и минимизировать падение напряжения по цепи питания, особенно в конце срока ее службы, когда возрастает внутреннее сопротивление (Rint на рисунке 8).

Беспроводная сеть

Беспроводной МК **CC2650** не сохраняет свое текущее состояние при переходе в спящий режим. По этой причине детектор газа предназначен для использования в сетях с топологией типа «звезда». Это означает, что каждый удаленный датчик соединяется непосредственно с центральным приемником, который принимает данные от датчика, а затем выполняет любую необходимую обработку и, в случае необходимости, соединяется с сетью верхнего уровня.

Это устройство не предназначено для использования в интеллектуальных ячеистых сетях. Встроенное ПО детектора рассылает пакеты из нескольких байт данных, содержащих информацию о концентрации CO, напряжении батареи, температуре и состоянии флагов.

В качестве приемопередающей антенны использована сформированная на печатной плате так называемая перевернутая F-антенна для диапазона 2,4 ГГц.

Контроль работы встроенного ПО

На рисунке 9 представлен алгоритм основного режима работы встроенного ПО детектора CO. Все начинается с проверки состояния пользовательской кнопки S1. Если кнопка нажата – встроенное ПО начинает процедуру калибровки. Если кнопка не нажата – ПО остается в состоянии ожидания. CC2650 в это время находится в спящем режиме для экономии электроэнергии.

Встроенное ПО будет находиться в состоянии ожидания до появления прерывания от компаратора или системного таймера. Если источником пробуждения будет системный таймер, начнется тестирование датчика. Если источником пробуждения будет компаратор, встроенное ПО переходит в состояние предварительной тревоги и будет контролировать уровень CO каждую секунду, используя 10-секундный интервал для усреднения выходного сигнала датчика CO.

Встроенное программное обеспечение переходит в состоянии тревоги, если концентрация CO превышает 65 ppm в течение минимального времени контроля, как указано в таблице 2. Встроенное ПО контролирует концентрацию CO каждую секунду и будет оставаться в состоянии тревоги, пока концентрация CO не упадет ниже 65 ppm.

Встроенное ПО будет периодически проверять исправность датчика и цепей ТИОУ, используя цепь самопроверки, и перейдет в состояние обслуживания “Trouble” (рисунок 10), если будет обнаружена ошибка. Если процесс тестирования системы пройдет успешно, выделяется 30 секунд для стабилизации показаний датчика, после чего отсылается пакет на хост с установленным в рабочее состояние флагом статуса, и ПО возвращается в состояние ожидания. Если будет обнаружена неисправность, прошивка переходит в состояние тревоги, в котором будет оставаться до

Таблица 2. **Концентрация CO и время отклика**

Концентрация, ppm	Время отклика, мин	
	Минимальное	Максимальное
70 ±5	60	240
150 ±5	10	50
400 ±5	4	15

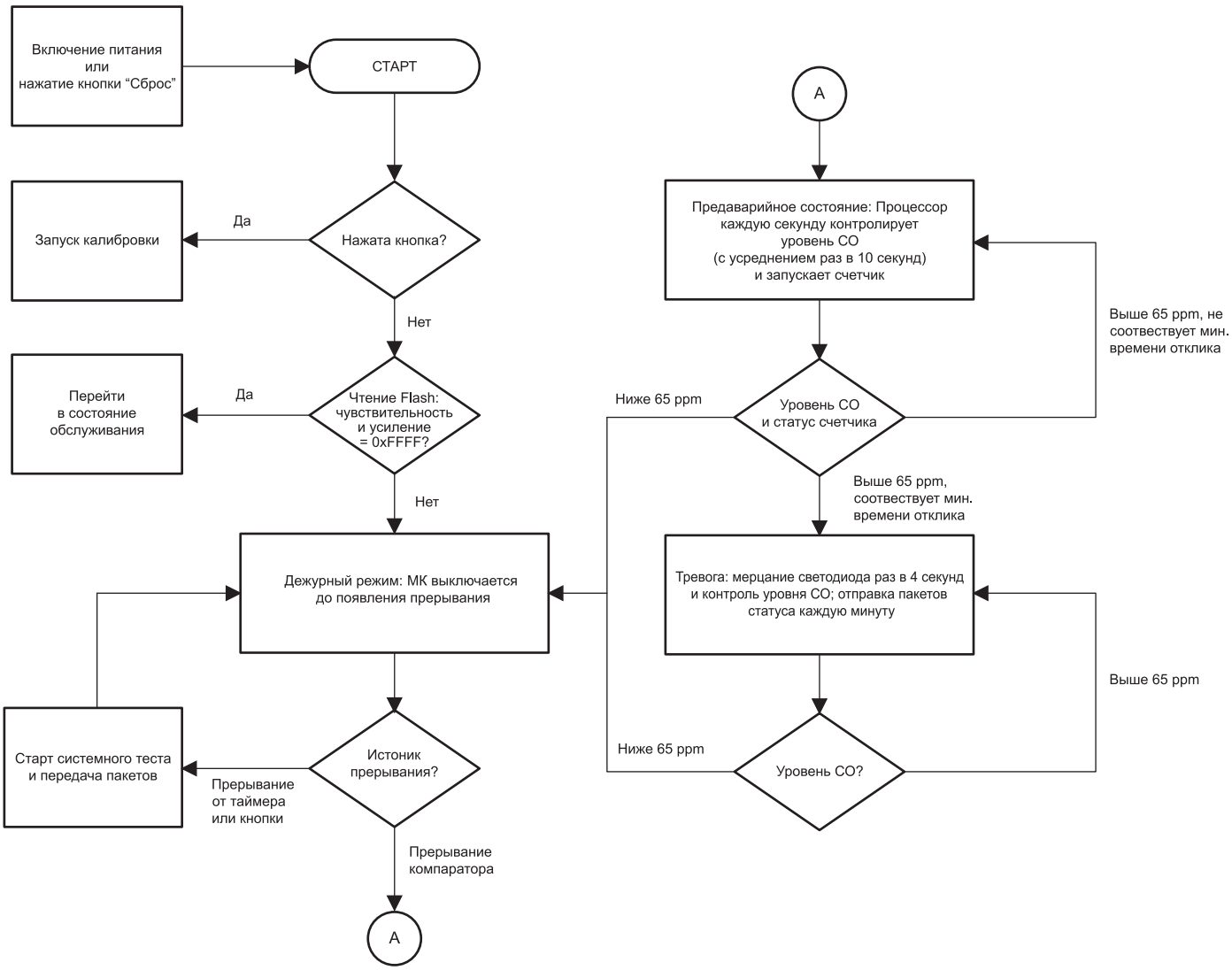


Рис. 9. **Блок-схема рабочего режима**

тех пор, пока система не будет сброшена. В состоянии тревоги будет непрерывно мигать светодиод, и каждую минуту будет отправляться пакет на хост со сброшенным флагом состояния.

Процедура калибровки позволяет пользователю настроить ряд параметров, включая чувствительность датчика и усиление ТИОУ. Все параметры сохраняются во Flash-памяти МК, откуда считываются и используются во время работы. Процедура калибровки инициируется после включения питания нажатием и отпускаем кнопки сброса при удерживаемой в нажатом состоянии кнопке S1.

Вся связь между аппаратными средствами и пользователем осуществляется через UART-интерфейс МК.

Последовательное соединение требуется для обмена данными с прошивкой во время процедуры калибровки.

Из процедуры калибровки пользователь может запустить измерение уровня CO с использованием сохраненной чувствительности и параметров усиления трансимпедансного усилителя. Поскольку UART-линии используются совместно с линиями I^2C, идущими к датчику температуры **TMP103,** передача показаний температуры в данном случае прекращается. Тем не менее, пользователь имеет возможность определения температуры. Показания тестовой температуры используются для выбора коэффициента коррекции температуры в процессе расчета уровня CO. Результат расчета выводится через последовательную консоль (рисунок 11).

Когда пользователь выйдет из программы калибровки, встроенное ПО перейдет в режим непрерывного отбора проб. В этом режиме каждую секунду будет передаваться пакет, содержащий уровень CO и температуру (таблица 3). Для выхода из режима непрерывного отбора проб потребуется аппаратный сброс.

Работа с аппаратным и программным обеспечением

Плата детектора

На рисунке 12 изображен наномощный детектор CO с поддержкой BLE, способный работать 10 лет от одной миниатюрной литиевой батареи. С нижней стороны по углам печатной платы размером 43×104 мм установлены нейлоновые стойки высотой 0,5″, чтобы упростить процедуру лабораторных измерений.

На верхней стороне печатной платы с четырехслойной разводкой сформирована так называемая. инвертированная F-антенна для работы в диапазоне до 2,4 ГГц. Здесь также размещены несколько тестовых точек и перемычек. Нижняя сторона платы включает держатель для батареи **CR2032.** Используемые во время калибровки два вывода **CC2650** выведены на контакты разъема J6. Эти выводы сконфигурированы как UART RX и TX для связи с хостом через последовательный порт во время калибровки.

На плате детектора предусмотрено несколько замыкаемых перемычек с возможностью изменения их конфигурации в процессе отладки и измерений. Необходимо следить за корректной установкой перемычек.

Конфигурация перемычек для нормальной работы выглядит следующим образом:

- J1 — замкнуто;
- J2 — замкнуто;
- J6 — разомкнуто;
- J8 — разомкнуто.

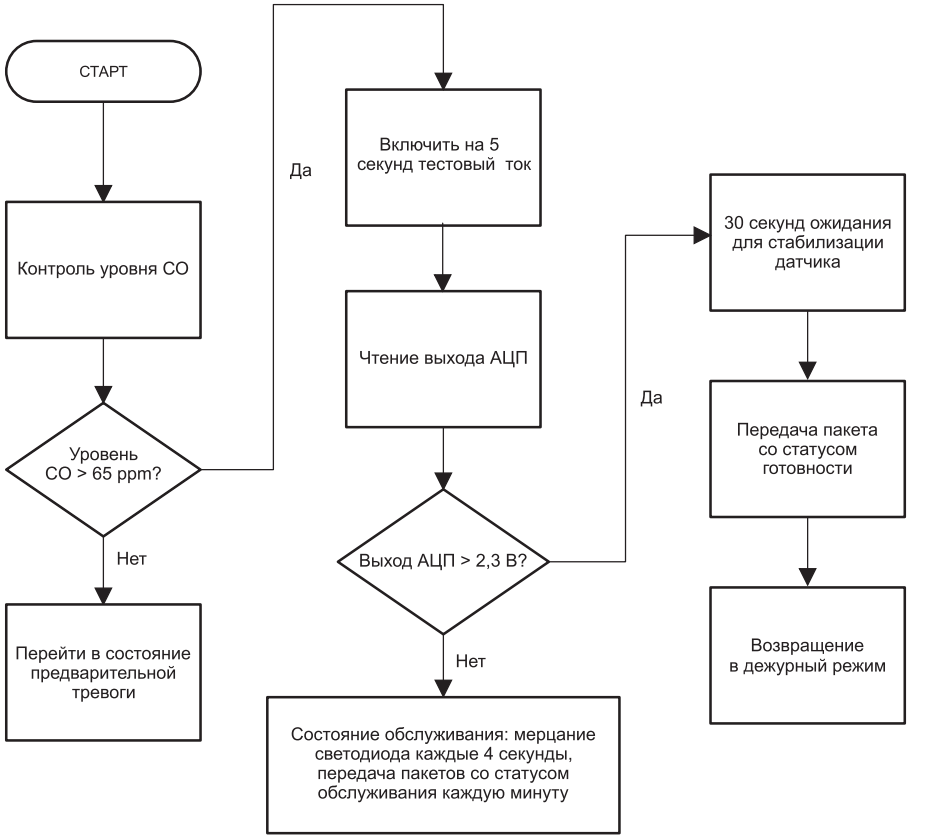


Рис. 10. **Блок-схема тестирования датчика и ТИОУ**

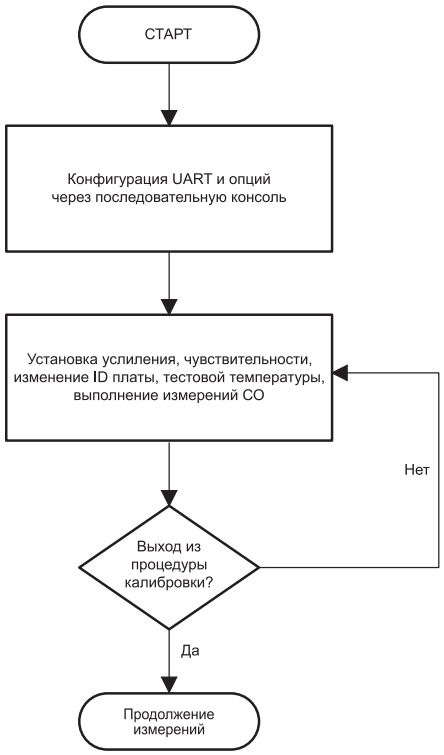


Рис. 11. **Блок-схема калибровки детектора**

Конфигурация перемычек для загрузки новой микропрограммы для CC2650 выглядит следующим образом:

- J1 — замкнуто;
- J2 — разомкнуто;
- J6 — разомкнуто;
- J8 подключается через ленточный кабель к 10-контактному разъему ARM Cortex Debug на оценочной плате **SmartRF06 (EVM).**

При подключении к оценочной плате (EVM) SmartRF06 установите на EVM-переключатель источника на USB и соедините перемычкой VDD с EM. В этой конфигурации EVM SmartRF06 обеспечивает питание CC2650.

При выполнении процедуры калибровки конфигурация перемычек выглядит следующим образом:

- J1 — замкнуто;
- J2 — замкнуто;
- J6 — подключено к хосту;
- J8 — разомкнуто.

Перемычка J6 выводит контакты CC2650 UART RX и TX. Эти контакты могут быть использованы для связи с компьютером посредством использования внешнего трансивера RS-232, например, **TTL-232R-3V3-PCB** производства компании **FTDI.**

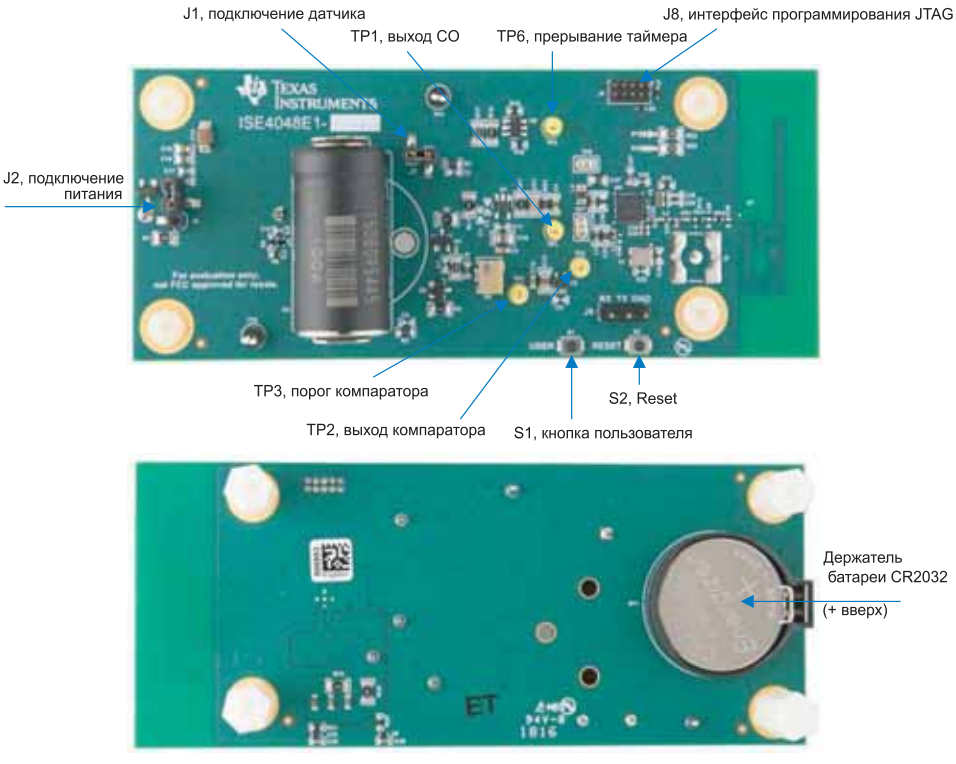


Рис. 12. **Плата детектора (вид сверху и снизу)**

Примечание. Убедитесь, что перевели плату в режим калибровки перед подключением внешнего приемопередатчика RS-232 на разъем J6.

На плате детектора предусмотрено несколько тестовых точек для контроля важных сигналов. Назначение тестовых точек следующее:

- TP1 — выход каскада ТИОУ и фильтра, который также является входом компаратора;
- TP2 — выход компаратора;
- TP3 — вход порогового напряжения для компаратора;
- TP4, TP5 — точки заземления для датчиков или общий провод для измерения напряжения;

Таблица 3. **Содержимое пакетов статуса**

Байты 0 и 1	Байт 2	Байт 3	Байты 4 и 5	Байт 6	Байты 7 и 8
Номер TIDA, по умолчанию 0x0738 или 756 в десятичном виде	ID платы	Флаги статуса: бит 0 – TROUBLE; бит 1 – ALARM; бит 2 – OK; бит 3 – CAL_ERROR; биты 4…7 – Резерв	Напряжение батареи	Температура	Концентрация CO

• TP6 – выход прерывания системного таймера;
• TP7 – вход конвертора DC/DC для отфильтрованного батарейного питания;
• TP8 – отфильтрованный выход конвертора DC/DC для CC2650.

Загрузка ПО

Для программирования детектора CO необходимо подключить ленточный кабель с 10-контактным разъемом между J8 и SmartRF06 (10-контактный разъем ARM Cortex Debug Connector, рисунок 13). На плате SmartRF06 установите переключатель источника USB и соедините перемычкой VDD с EM. В этой конфигурации EVM SmartRF06 обеспечивает питание CC2650. Перед подачей напряжения питания установите соответствующим образом все перемычки. Дополнительную информацию можно получить из документации к SmartRF06.

После полной настройки оборудования выполните следующие действия, чтобы загрузить новую версию прошивки детектора CO с помощью программы SmartRF Flash Programmer 2:

• Скачайте и установите SmartRF Flash Programmer 2 (*http://www.ti.com/tool/flash-programmer*).
• Откройте SmartRF Flash Programmer 2.
• В окне «Connected devices» CC2650 должен быть под строкой XDS100v3. Если его нет в списке – проверьте питание и подключение от SmartRF06 к TIDA-00756 и нажмите кнопку «Обновить» для повторного сканирования устройств. Выделите устройство CC2650 (рисунок 14).
• На вкладке «Main» нажмите кнопку «Single».
• ВАЖНО: На вкладке «Main» в разделе «Actions» выделите кнопку «Pages in image». Это предотвратит стирание каких-либо значений калибровки, ранее записанных во Flash-память.
• Нажмите на кнопку “Browse” и перейдите к файлу TIDA00756-Firmware.out.
• Нажмите на синюю круглую кнопку воспроизведения, чтобы записать прошивку на плату TIDA-00756. Строка состояния в нижней части SmartRF Flash Programmer 2 отобразит успешность записи.

Прием пакетов данных

Встроенное ПО детектора призвано контролировать уровень CO и периодически оценивать состояние системы. Периодически CC2650 передает по сети пакеты данных для взаимодействия с основным узлом.

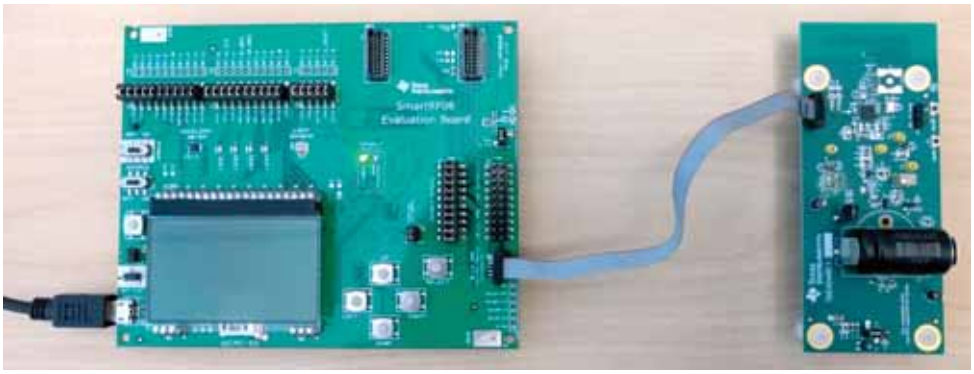


Рис. 13. **Подключение EVM SmartRF06 к детектору CO для программирования и отладки**

Рис. 14. **Конфигурация SmartRF Flash Programmer 2**

Существует два способа просмотра передаваемых пакетов.

Прием пакетов данных с использованием CC2540EMK-USB и протокол SmartRF Sniffer: с целью контроля работы радиопередатчика используется оценочный модуль CC2540EMK-USB для перехвата с помощью программного перехватчика SmartRF Protocol Packet Sniffer. После установки ПО перехватчика пакетов (v2.18.1 на момент написания статьи) процедура контроля передаваемых данных выглядит следующим образом:

• Подключите CC2540EMK-USB в неиспользуемый порт USB на компьютере с установленным программным обеспечением Packet Sniffer.
• Откройте программу Packet Sniffer, выберите «Bluetooth Low Energy» в качестве протокола и нажмите кнопку “Start” (рисунок 15).
• Выберите вкладку Radio Configuration и убедитесь, что выбрано «Advertising Channel 39».
• Нажмите вверху на панели инструментов кнопку “Play”, чтобы инициировать процесс захвата пакетов.
• Возможно, будет обнаружено множество пакетов, передаваемых с разных устройств, использующих про-

Рис. 15. **ПО Packet Sniffer**

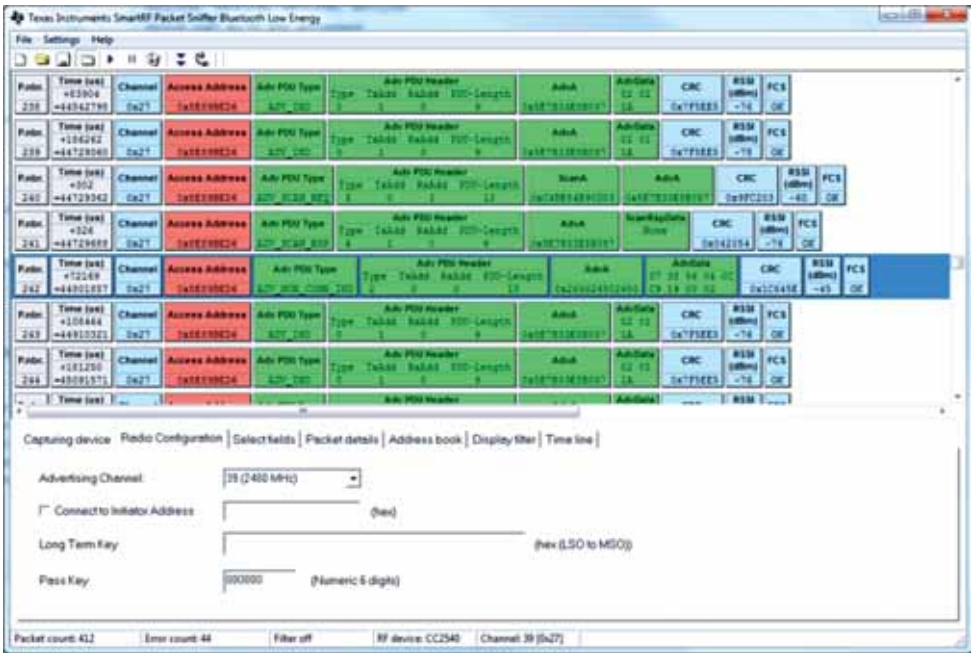


Рис. 16. **Общий список пакетов на экране Packet Sniffer**

токол Bluetooth Smart, включая мобильные телефоны. Подсвеченная строка включит нужный пакет данных в общем перечне. На рисунке 16 приведен пример неотфильтрованного перечня пакетов.

• Для выделения пакетов, отправленных с детектора CO, необходимо применить фильтр отображения. Соответствующий фильтр для так называемых пакетов объявления (advertisement packets) задается в поле “ADV_NONCONN Adva” значением 0x265026502650. В поле “Field Name” выберите “ADV_NONCONNADVA” из выпадающей опции. Нажмите кнопку «First». Измените условия фильтра на нужный адрес, нажмите кнопку «Add» и затем «Apply filter». Пример отфильтрованного списка показан на рисунке 17.

• Чтобы экспортировать захваченные отфильтрованные пакеты, нажмите кнопку «Saves the current session» на панели инструментов или поставьте на паузу захват пакетов и нажмите Файл → Сохранить данные… Любой из этих вариантов предложит сохранить отображаемые данные в виде файла анализатора пакетов данных (.psd).

• Конвертируйте файл .psd с помощью программного обеспечения HexEdit в файл с шестнадцатеричными значениями. Другой редактор также может выполнять эту задачу.

• Откройте файл .psd в программном обеспечении HexEdit. Нажмите Tools → Options. В окне “HexEdit Options” нажмите Document → Display и измените значение “Columns value” на 271. Нажмите Edit → Select All и Edit → Copy As Hex Text. Откройте текстовый редактор (например, «Блокнот»), вставьте шестнадцатеричный текст и сохраните текстовый файл. Его можно импортировать в электронную таблицу Microsoft Excel для дальнейшего анализа.

Для второго метода используйте SmartRF06 Evaluation Board и оценочный модуль CC2650 Evaluation Module для контроля передаваемых пакетов с применением программы SmartRF Studio.

Загрузка калибровочных данных

Есть два метода загрузки калибровочных данных в детектор CO. Первый использует процедуру калибровки, запрограммированную в прошивке устройства. Для использования этого метода потребуется внешний приемопередатчик RS-232. Второй метод использует Flash Programmer 2, чтобы загрузить значения калибровки непосредственно в память детектора.

Загрузка данных с помощью процедуры калибровки: детектор CO поддерживает процедуру калибровки, с помощью которой пользователь может выполнять такую функцию как настройка чувствительности датчика CO и коэффициента усиления ТИОУ. Для использования процедуры калибровки выполните следующие шаги:

Сконфигурируйте перемычки на плате:

• J1 — замкнуто;
• J2 — замкнуто;
• J6 — подключено к хосту через внешний приемопередатчик RS-232, например, TTL-232R-3V3-PCB для FTDI;
• J8 — разомкнуто.
• Подключите плату к последовательному порту хост-компьютера.
• Откройте на хост-компьютере последовательный терминал (например, Tera Term) со следующими параметрами:
— скорость передачи: 115200;
— размер данных: 8 бит;
— стоповые биты: 1;
— проверка на четность: нет;
— управление потоком: нет.
• Включите питание платы.
• Удерживайте нажатой кнопку S1 при отпускании кнопки сброса S2.
• Следуйте инструкциям на последовательном терминале для завершения процедуры калибровки.

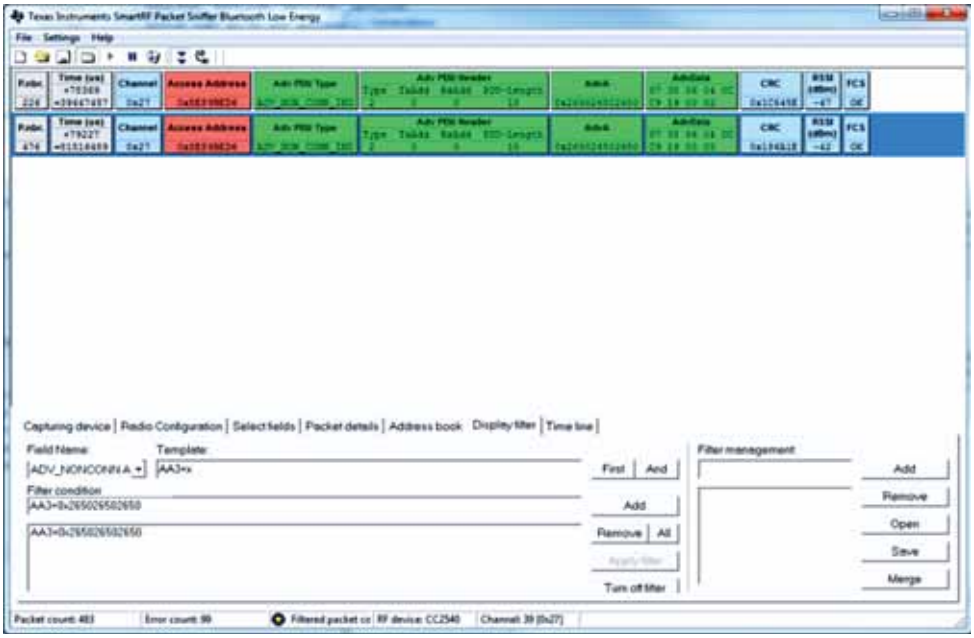


Рис. 17. **Отфильтрованный список пакетов на экране Packet Sniffer**

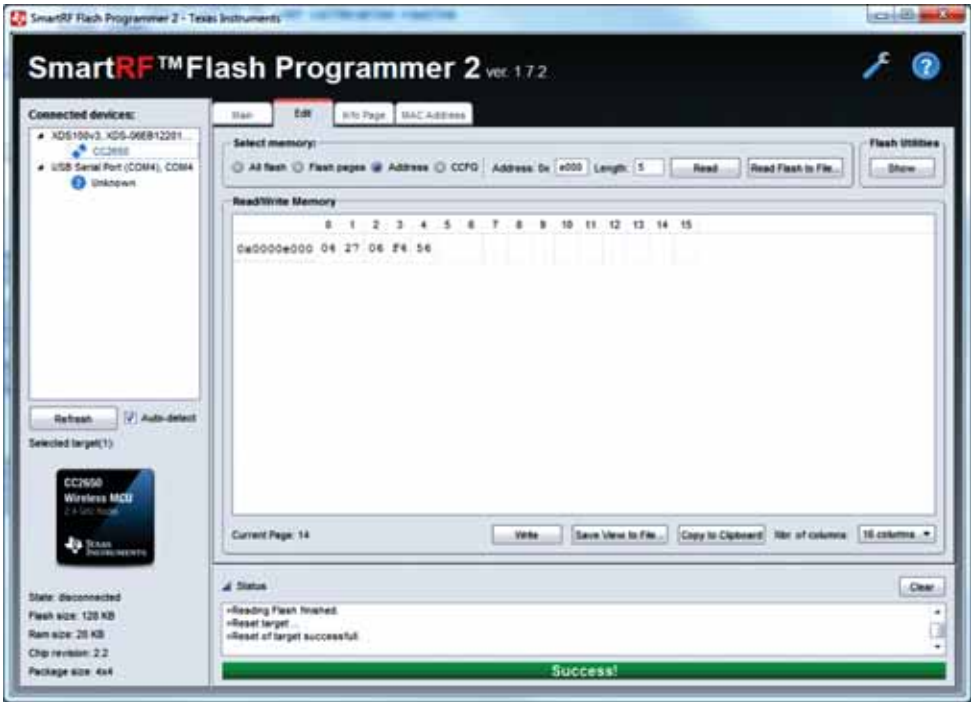


Рис. 18. **Конфигурация SmartRF Flash Programmer 2 для загрузки калибровочных данных**

Примечание: убедитесь, что перевели плату в режим калибровки перед подключением внешнего приемопередатчика RS-232 к разъему J6.

Загрузка данных с помощью Flash Programmer 2: выполните следующие действия, чтобы загрузить новые значения калибровки для детектора CO, используя SmartRF Flash Programmer 2:

- Загрузите и установите SmartRF Flash Programmer 2 со страницы *http://www.ti.com/tool/flash-programmer*.
- Откройте SmartRF Flash Programmer 2.
- В окне «Connected devices» CC2650 должен быть под строкой XDS100v3. Если его нет в списке — проверьте питание и подключение от SmartRF06 к TIDA-00756 и нажмите кнопку «Обновить» для повторного сканирования устройств. Выделите устройство CC2650.
- На вкладке «Edit» в разделе «Select memory» нажмите кнопку «Address» и введите адрес «E000» и длину «5».
- Нажмите на кнопку «Read».
- Произойдет обновление пяти байтов с новыми значениями калибровки в шестнадцатеричном формате:

— байт 0 — чувствительность датчика, MSB;
— байт 1 — чувствительность датчика, LSB;
— байт 2 — усиление, MSB;
— байт 3 — усиление, LSB;
— байт 4 — идентификатор платы.

- Нажмите кнопку «Write'
- Строка состояния в нижней части SmartRF Flash Programmer 2 отобразит успешность записи (рисунок 18).

Заключение

Проблемы электропитания создают одни из наиболее серьезных ограничений для беспроводной сети с использованием удаленных датчиков. Поскольку эти устройства питаются от батарей, расходы на техническое обслуживание, включающее периодическую замену элементов питания, порой, могут оказаться неоправданно высокими.

Аналоговые компоненты с энергопотреблением на уровне наноампер и сверхэкономичная микроконтроллерная платформа TI SimpleLink с поддержкой целого ряда беспроводных стандартов позволили компании Texas Instruments разработать суперэкономичный, беспроводной детектор непрерывного контроля уровня концентрации окиси углерода в воздухе для применения в промышленности, в быту и на транспорте.

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

Кумаран Виджаясанкар, Роберто Сандре (Texas Instruments)

СКАЧКООБРАЗНАЯ ПЕРЕСТРОЙКА ЧАСТОТЫ В СЕТЯХ IOT

Программный продукт 15.4-Stack SDK, *разработанный* ***Texas Instruments,*** *предназначен для повышения надежности беспроводных сетей* ***Интернета вещей.*** *Он реализует псевдослучайную* ***перестройку частоты*** *в каналах обмена данными, что существенно* ***повышает помехоустойчивость.***

Использование беспроводных технологий связи в системах управления и безопасности немыслимо без надежного протокола обмена данными с высокой достоверностью передачи сообщений внутри сети. Упростить решение этой задачи призван созданный компанией **Texas Instruments** программный продукт TI 15.4-Stack SDK, реализующий механизм псевдослучайной перестройки рабочей частоты, оценку занятости канала, подтверждение об успешной доставке пакета и автоматическую повторную отправку сообщений.

Технологии дистанционного управления оборудованием и взаимообмена данными через Интернет, известные как Интернет вещей (IoT), открывают целый ряд возможностей на основе встраиваемых и подключаемых к сети устройств. Это позволяет упростить управление, повысить безопасность и расширить функциональность. Комплект для разработки программного обеспечения (SDK) производства компании TI **15.4-Stack** предоставляет основанный на стандартах 802.25.4 протокол доступа к среде (MAC), отлично подходящий для создания облачных беспроводных приложений. Рабочий проект для построения сети из координатора и множества беспроводных датчиков включен в состав SDK.

Вот лишь некоторые из основных применений для этого программного решения

- Автоматизация зданий

– системы охраны: дверные и оконные датчики, инфракрасные датчики, гаражные ворота и многое другое;

– системы пожарной безопасности: датчики газа и дыма;

– системы вентиляции и кондиционирования: датчики воздуха, влажности, температуры, воды и сигнализаторы утечки.

- Автоматизация производства

– измерительные преобразователи: датчики потока, давления и другие;

– управление технологическим процессом: гидравлические и пневматические клапаны.

- Прочее промышленное оборудование

– управление доступом, контроль перемещений объектов, торговое оборудование.

- Интеллектуальные сети и возобновляемая энергетика

– счетчики газа, воды, электроэнергии, тепла.

Для подобных беспроводных систем часто требуется расширенная зона действия с защитой от помех, возникающих на рабочих частотах. Дальность связи в диапазоне 2,4 ГГц крайне ограничена и требует использования ячеистой сети или маршрутизации на верхнем уровне, чтобы охватить большую территорию. Это усложняет систему и увеличивает ее общую стоимость, повышает энергопотребление и задержки при передаче сигнала.

Предлагаемое компанией TI решение 15.4-Stack SDK, созданное на базе микроконтроллера **SimpleLink CC1310,** как раз и решает данную проблему, предоставляя стандартный MAC-стек и обеспечивая расширенную зону действия благодаря работе в диапазонах до 1 ГГц. В дополнение, TI 15.4-Stack SDK также поддерживает Frequency Hopping – режим скачкообразной перестройки частоты (СПЧ). Режим СПЧ построен на базе беспроводной спецификации альянса Wi-SUN для локальных сетей FAN (*Field Area Networks*).

Функция СПЧ позволяет устройствам вести прием и передачу по нескольким каналам. Это позволяет расширить зону действия беспроводной сети при полном соответствии требованиям Федеральной комиссии по связи (FCC). Кроме того, скачкообразная перестройка частоты решает проблему помех на определенных рабочих каналах. Увеличение практической дальности связи позволяет во многих случаях ограничиться простой топологией сети типа «звезда». Отсутствие ретрансляций и простая адресация повышают общую надежность беспроводной системы.

Механизм прыгающих частот

Скачкообразная перестройка частоты обеспечивается за счет смены устройством канала приема в процессе работы. Последовательность смены частотных каналов основана на прямой хэш-функции номера канала (DH1CF), как определено в спецификации Wi-SUN FAN. Функция DH1CF генерирует псевдослучайную последовательность рабочих каналов на основе расширенного (*extended*) адреса узла сети и, следовательно, она является уникальной для каждого узла. Каждый узел поддерживает два типа последовательностей скачкообразной перестройки частоты канала: адресную (*Unicast*) при обращении к конкретному устройству и широковещательную (*Broadcast*) рассылку для всех устройств в сети.

Каждый узел меняет частоту на основе собственной уникальной последовательности перебора каналов при адресной передаче (рисунок 1). При широковещательной передаче координатор запускает график оповещения, как показано на рисунке 2. Каждое устройство будет следовать полученному от координатора порядку перебора частотных каналов. Между широковещательными пакетами от координатора устройство будет выполнять свою одноадресную СПЧ. Затем оно переключится на широковещательный канал СПЧ и возобновит одноадресную СПЧ по завершении периода Broadcast Dwell.

Используемое каждым каналом время контролируется через параметр, на-

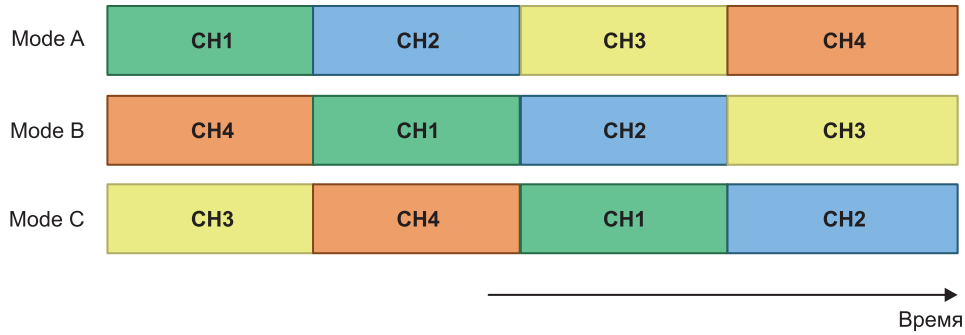


Рис. 1. **Последовательность одноадресной СПЧ**

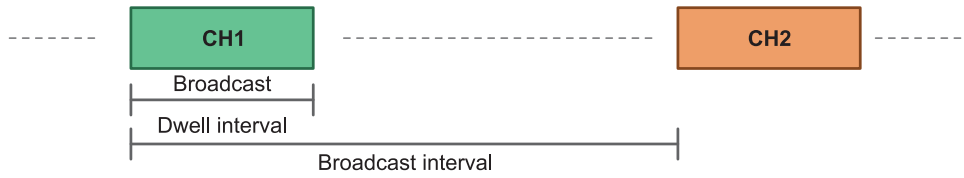


Рис. 2. **Последовательность СПЧ широковещательного канала**

зываемый периодом Dwell, который может быть настроен пользователем в пределах 15…250 мс. Информацией о последовательности частотных скачков узлы обмениваются друг с другом во время процедуры начального обнаружения (*discovering*) и соединения (*joining*), выполняемых с помощью асинхронных передач. Как только информация о СПЧ соседнего узла будет получена, TI 15.4-Stack SDK начинает отслеживать частотные скачки соседних устройств и делает возможными адресные и широковещательные передачи. Обмен данными обеспечивается передатчиком, передающим фреймы данных на текущем рабочем частотном канале узла-приемника (прямая передача приемнику).

Режим сна

TI 15.4-Stack SDK также поддерживает фирменные режимы сна с использованием непрямой передачи (*indirect transmission*) в соответствии со стандартом IEEE 802.15.4. В этом режиме работы TI 15.4-Stack SDK конфигурируется для работы на одном фиксированном частотном канале. Актуальный используемый канал может быть в дальнейшем изменен пользователем (с учетом интервалов опроса координатора конечными устройствами). Это обеспечивает для пользователя расширенный контроль за сменой частот и временем операций. TI 15.4-Stack SDK позволяет отслеживать перестройку частотных каналов координатора даже в периоды сна. Поддерживаются периоды сна до 25 минут, при этом все еще обеспечивается эффективное отслеживание последовательности СПЧ координатора. Это позволяет работать при чрезвычайно низком потреблении энергии.

Требования по электромагнитной совместимости

Использование спектра радиочастот и мощности радиопередатчиков строго контролируется специально уполномоченными национальными органами. В России это Государственный комитет по радиочастотам (ГКРЧ), в США — Федеральная комиссия по связи (FCC). Согласно уже действующим нормам американского регулятора, определены требования к системам, использующим технологию СПЧ, которые могут использовать повышенную мощность радиопередачи, в сравнении с другими системами, не использующими СПЧ.

Эти нормы также определяют среднее время занятия частотного канала. При использовании СПЧ передача на отдельно взятой частоте занимает меньше времени, что позволяет использовать более высокую мощность передачи. Повышенная мощность передатчика подразумевает большую дальность связи, что может быть крайне полезно как для промышленных систем, так и для городского использования интеллектуальных беспроводных технологий. Использование СПЧ с соблюдением норм FCC позволяет расширить площадь зоны действия беспроводных систем до 34 раз в сельской местности и до 13 раз — в городских районах.

Влияние помех

Помимо обеспечения большей дальности, скачкообразно перестраиваемая частота также может быть эффективным инструментом в обеспечении надежной связи даже при наличии помех. Поскольку обмен данными осуществляется на разных частотных каналах, как правило, пакет данных должен успешно добираться до места назначения. Возможна также настройка конфигурации с исключением тех частотных каналов, на которых предположительно могут возникнуть помехи. Однако когда подверженные помехам каналы заранее не известны или могут изменяться со временем, предварительно запрограммированное исключение каналов может не сработать. В таких случаях может помочь скачкообразная перестройка частоты.

Помехозащищенность может быть повышена за счет увеличения количества каналов и/или добавления повторных передач на уровне приложений. Для изучения влияния помех SDK TI 15.4-Stack включает пример сети с двумя узлами. Этот пример включает два типа трафика: 1 — сообщения от датчика (Sensor messages, периодически передающиеся от датчика к коллектору) и 2 — контрольные сообщения (Tracking messages, передаваемые от коллектора к датчику, используя непрямые передачи). В процессе практического тестирования помехи по четырем определяемым каналам вносятся с помощью радиочастотного приемопередатчика TI **CC1200** на базе оценочной

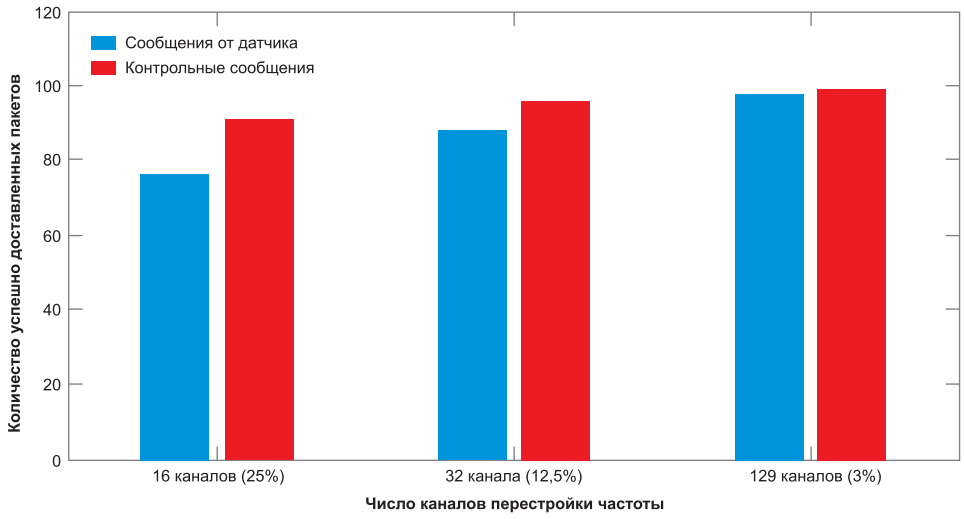


Рис. 3. **Повышение надежности при увеличении количества каналов СПЧ**

платы **SmartRF.** Помехи, как предполагается, появляются после запуска сети и, следовательно, невозможно предварительно блокировать какой-то канал заранее, то есть во время выбора канала при запуске сети.

В сетях, не использующих СПЧ, работа будет нарушена из-за постоянных помех. Нормальное функционирование сети должно быть восстановлено с переходом на другой канал с использованием методов прикладного уровня. Однако в случае применения СПЧ MAC автоматически использует несколько каналов и таким образом помогает преодолеть помехи. Рисунок 3 иллюстрирует повышенную устойчивость к помехам при увеличении числа каналов СПЧ. Из него видно, что успешность передачи сообщений от собирающих данные датчиков пропорциональна уровню помех. А контрольные сообщения немного более устойчивы к помехам за счет использования нескольких попыток опроса. Как можно заметить, помехи могут быть сведены к минимуму путем увеличения количества каналов СПЧ.

Рисунок 4 иллюстрирует устойчивость к помехам, которая может быть достигнута с помощью повторных передач на уровне приложений. Допустима ретрансляционная задержка длительностью 1…3 с. В системах с СПЧ повторно передаваемый кадр будет отправлен по разным каналам, что обычно приводит к успешной доставке в обход каналов, подверженных помехам.

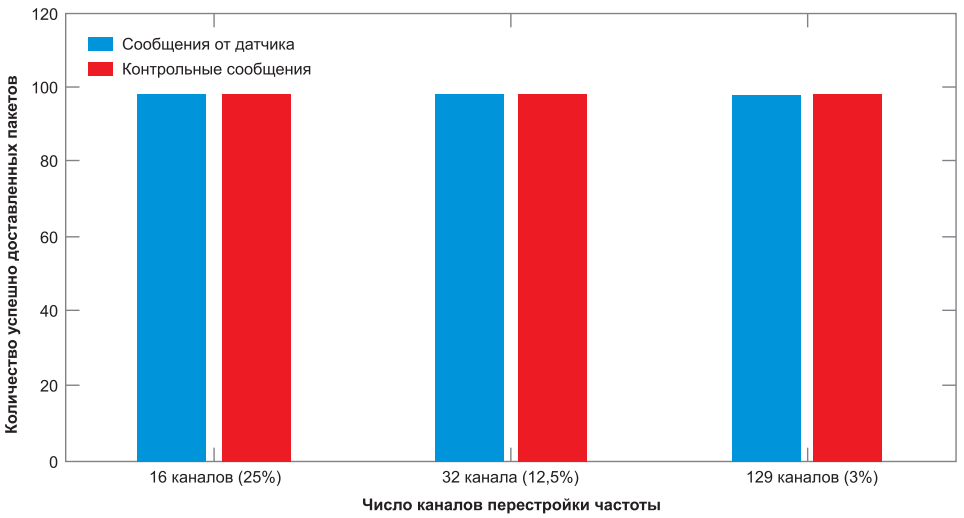


Рис. 4. **Повышение надежности на уровне приложений за счет повторных передач**

Заключение

TI 15.4-Stack SDK предлагает протокол для построения беспроводных сетей повышенной надежности, в том числе и со спящими конечными узлами. Благодаря использованию технологии псевдослучайной перестройки частоты предлагаемое решение является более устойчивым к помехам, которые могут возникать на отдельных частотных каналах. Использование диапазона ниже 1 ГГц обеспечивает расширенную зону действия системы. Увеличенная дальность связи помогает решать специфические задачи в таких сегментах рынка как автоматизация зданий, автоматизация производства и приложения для интеллектуальных сетей.

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

life.augmented

Контролируй это!

Инновационные датчики STMicroelectronics и библиотеки для работы с ними

- 6-осевой МЭМС-датчик для навигационных приложений LSM6DS3
- Лазерные датчики измерения расстояния VL6180 и VL53L0x
- Датчики атмосферного давления с защитой от влаги LPS35H/LPS25HTR
- МЭМС-микрофоны MP23xx/MP33xx и библиотека направленного звука
- Цифровой датчик температуры и влажности HTS221TR
- Библиотека для обработки данных с МЭМС-датчиков SensorFusion osxMotionFX

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

Компэл
www.compel.ru