

«Элиот» – система на кристалле для Интернета вещей

Я. Петричкович, д. т. н.¹, Т. Солохина, к. т. н.¹, Д. Кузнецов¹,
Л. Меньшенин¹, Ф. Путря, к. т. н.¹, А. Функнер¹, Е. Белогубцев¹,
Е. Гришаев¹, Е. Омелянчук¹, С. Фролова¹, С. Лавлинский¹, С. Груздев²

УДК 004.318 | ВАК 05.27.01

Кевин Эштон (Kevin Ashton), основоположник концепции Интернета вещей (Internet of Things, IoT), следующим образом определил понятие IoT: «Если в 20 веке данные попадали в компьютер только от человека, использовавшего для их ввода дополнительные устройства, то в 21 веке мы уже имеем дело с гаджетами, которые сами могут собирать и отправлять данные. В этом и состоит суть Интернета вещей. Данные собираются, обрабатываются и передаются устройствами без участия человека». Компания Arm прогнозирует, что интенсивность обмена данными между IoT-устройствами в 2021 году достигнет миллиардов транзакций. В рамках реализации отечественной стратегии «от периферии к облаку» в АО НПЦ «ЭЛВИС» разработана система на кристалле (СнК) «Элиот», предназначенная для применения в условиях ограниченного энергопотребления и обеспечения доверенности в IoT-сетях. В статье представлены архитектурные особенности, ключевые характеристики, основные области применения новой СнК.

КЛЮЧЕВЫЕ ОСОБЕННОСТИ СнК «ЭЛИОТ»

Микросхема «Элиот» (1892ВМ268) разработана в дизайн-центре АО НПЦ «ЭЛВИС» и представляет собой малопотребляющую 2-ядерную СнК, которая, в первую очередь, предназначена для применения в качестве микроконтроллера для устройств Интернета вещей и поддержки концепции «от периферии к облаку». СнК изготовлена на фабрике TSMC по малопотребляющему (ultra-low power, ulp) 40-нм процессу и содержит 34 млн транзисторов на кристалле площадью 11,66 мм².

Микросхема, в общей сложности, содержит 30 типов IP-ядер (процессорных, периферийных и др.). Ряд ключевых IP-ядер является собственной разработкой компании, в том числе ядро малопотребляющего контроллера цифровой части приемника навигационного сигнала Navicore S с поддержкой стандартов ГЛОНАСС/GPS, специально адаптированное для IoT-применений, а также блоки для реализации решений информационной безопасности.

СОСТАВ СнК «ЭЛИОТ»

СнК «Элиот» имеет 2-процессорную архитектуру Arm с поддержкой операций с плавающей точкой (FPU) на одном из процессорных ядер (рис. 1).

Вычислительный кластер содержит два ядра Arm Cortex-M33 (архитектура Arm v8M, технология Arm TrustZone): энергоэффективное ядро CPU0 с максимальной частотой 50 МГц и быстродействующее ядро CPU1 с максимальной частотой 160 МГц (с расширениями DSP и FPU). Каждое ядро содержит кэш инструкций размером 16 Кбайт.

Блок крипто-акселераторов Arm Crypto Cell (CC) обеспечивает поддержку алгоритмов шифрования AES, Stream Ciphers, RSA, DH, ECC, а также поддержку HASH и HMAC. В состав блока входит генератор истинно случайных чисел (True Random Number Generator, TRNG). Задачами Arm Crypto Cell (CC) являются также обеспечение доверенной загрузки и отладки, а также реализация функций управления жизненным циклом системы.

В состав вычислительного кластера входит также блок акселерации программно-определяемых криптографических алгоритмов ГОСТ GMS Crypto (GMS). Приемник сигналов систем спутниковой навигации (GNSS) обеспечивает прием навигационного сигнала СТ системы ГЛОНАСС и навигационного сигнала СА системы GPS.

В **подсистему памяти** входят четыре независимых банка памяти SRAM 0–3 общим объемом 320 Кбайт: SRAM0 – 128 Кбайт, SRAM1–3 – по 64 Кбайт каждый. Банки SRAM0–2 работают на частоте SYSCLK, банк SRAM3 – на частоте FCLK (частота CPU1). Независимо

¹ АО НПЦ «ЭЛВИС».

² АО «Аладин Р.Д.».

для каждого банка реализована поддержка малопотребляющих режимов с сохранением данных (retention) и полного выключения (shutdown). В батарейном режиме предусмотрен дополнительный блок памяти размером 1 Кбайт.

СНК оснащена встроенной флеш-памятью с размером страницы 8 Кбайт: объем основного раздела составляет 640 Кбайт, системного раздела – 32 Кбайт, дополнительный флеш-кэш размером 8 Кбайт. Однократно программируемая память (OTP) объемом 1 Кбайт используется для хранения ключей, пользовательских данных и доверенного начального загрузчика, обеспечивающего контроль целостности и подлинности встроенного программного обеспечения. СНК оснащена также двумя системными контроллерами прямого доступа в память (DMA).

В состав СНК входит набор **таймеров и сенсоров**, в том числе таймер реального времени (RTC), сторожевые таймеры (WDT, LPWDT), таймеры общего назначения (TIM0, TIM1 DTIM, LPTIM), блок генерации ШИМ-сигналов (PWM), а также многофункциональный таймер (VTU), реконфигурируемый как: два 8-разрядных или один 16-разрядный генератор ШИМ-сигнала, или 16-разрядный счетчик с двумя каналами захвата. Кроме того, имеются встроенные сенсоры температуры и напряжения.

В состав **периферии** входят: интерфейс USB 2.0 OTG (до 480 Мбит/с), интерфейс CAN (CAN 2.0B, CAN FD, скорость до 1 Мбит/с), четыре интерфейса GPIO (16 линий на канал), четыре интерфейса UART, два интерфейса I2C (до 3,4 Мбит/с), интерфейс I2S, три интерфейса SPI, интерфейсы для подключения внешней памяти: интерфейс Quad SPI (QSPI), интерфейс внешней статической памяти (SMC), поддержка до двух микросхем памяти SRAM, PSRAM, NOR-флеш памяти общим объемом до 64 Мбайт, поддержка NAND-флеш памяти с интерфейсом SRAM.

Кроме того, СНК оснащена интерфейсом SD/SDIO/MMC, обеспечивающим подключение карт памяти.

Для обеспечения вывода трассы, а также безопасной / доверенной отладки с управлением доступа к различным ресурсам системы в состав СНК введен отладочный интерфейс JTAG / Serial Wire Debug.

НАВИГАЦИОННОЕ РЕШЕНИЕ В СНК «ЭЛИОТ»

В компании «ЭЛВИС» разработана мультистандартная технология навигации (ГЛОНАСС/GPS/BEIDOU/GALILEO), которая отличается повышенной гибкостью. Она состоит из семейства IP-ядер аппаратного ускорителя GNSS (Navicore), IP-ядра радиочастотного приемника RF GNSS (RF Front-End) и библиотеки ПО GNSS-приемника. Комплекс программно-аппаратных средств по интегральным параметрам GNSS-приемника соответствует мировому уровню.

В СНК «Элиот» входит малопотребляющее, специально адаптированное для IoT-применений, двухсистемное ГЛОНАСС/GPS IP-ядро аппаратного ускорителя Navicore-S, содержащее 20 следящих каналов и устройство быстрого поиска (Fast Search Engine, FSE). Наличие навигационного IP-ядра является одним из преимуществ СНК «Элиот» на рынке IoT-микросхем, что позволяет реализовывать на нем устройства для задач мониторинга и слежения за подвижными объектами, выполняя шифрацию навигационных данных непосредственно внутри СНК.

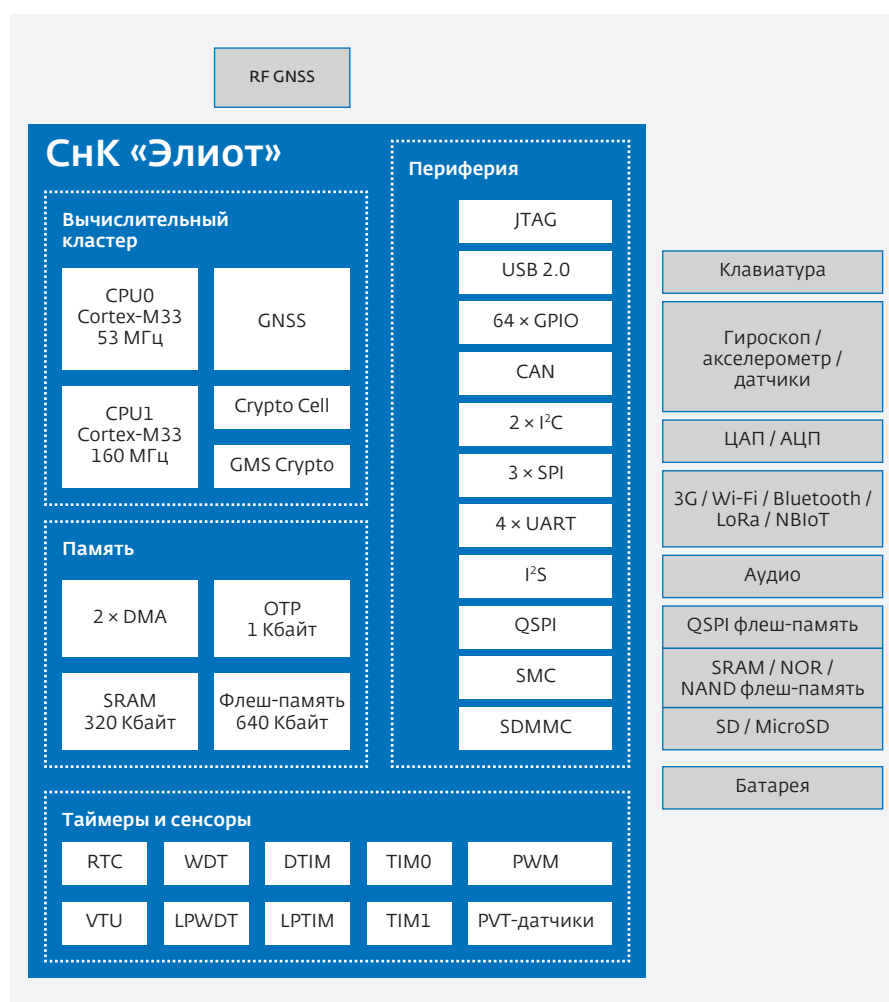


Рис. 1. Структура СНК «Элиот»

IP-ядро RF GNSS предназначено для приема сигналов GPS и ГЛОНАСС в диапазоне L1 и позволяет обеспечить одновременный прием сигналов указанных систем. Ядро обеспечивает высокую чувствительность (-148 дБм) при низком потреблении (90 мВт против 150 мВт у импортных аналогов). Выигрыш в потреблении осуществляется за счет использования одного синтезатора для приема двух систем. Ядро предназначено для построения как отдельной микросхемы RF FE, так и СМК и систем в корпусе.

Навигационное ПО GNSS исполняется на ядре CPU0. В режиме разделения задач ядро CPU0 недоступно для исполнения пользовательских программ, для пользовательских приложений остается доступным CPU1. В навигационном ПО применяются современные оптимизированные алгоритмы обработки сигналов, которые обеспечивают превосходные навигационные характеристики GNSS-приемника. Оптимальная реализация выбранных алгоритмов обработки позволяет использовать навигационный приемник на облегченных вычислительных ядрах без видимого ухудшения потребительских характеристик навигационного решения.

Применяемый в СМК «Элиот» комплекс аппаратно-программных средств обеспечивает следующие интегральные характеристики навигационного приемника:

- поддерживаемые системы: ГЛОНАСС / GPS L1;
- чувствительность холодного старта: до -151 дБм;
- чувствительность слежения: до -162 дБм;
- время холодного старта (при уровне сигнала не ниже -130 дБм): 25 с;
- время горячего старта (при уровне сигнала не ниже -130 дБм): 1 с.

Системные требования для ПО GNSS:

- требуемый объем памяти инструкций: 350 Кбайт;
- требуемый объем памяти данных: 250 Кбайт;
- минимальная частота CPU: 50 МГц.

КОНТУРЫ ЗАЩИТЫ ИНФОРМАЦИИ В СМК «ЭЛИОТ»

Защита информации является одним из важнейших требований безопасности эксплуатации IoT-сетей и IoT-приложений в мире.

В СМК «Элиот» реализованы три контура защиты:

- **нулевой контур**, реализующий корень доверия, обеспечивает начальную инициализацию СМК и доверенную загрузку;
- **первый контур** использует уникальные возможности технологии Arm TrustZone для размещения в защищенной области памяти СМК модуля обеспечения безопасности;
- **второй контур** основан на использовании в составе СМК высокоскоростной программной криптографии (поддержка международных и отечественных стандартов) с аппаратной акселерацией.

Аппаратные возможности микросхемы поддержаны программными средствами обеспечения информационной безопасности от компании-партнера АО «Аладдин Р.Д.». В качестве начального загрузчика доступен модуль инициализации и доверенной загрузки TSM-M. В качестве модуля безопасности для Arm TrustZone возможно использование отечественного доверенного модуля с поддержкой сертифицированной российской криптографии Aladdin Secure Firmware (от компании «Аладдин Р.Д.»).

Аппаратная платформа от АО НПЦ «ЭЛВИС» и ПО безопасности от «Аладдин Р.Д.» является законченным программно-аппаратным решением и могут быть сертифицированы на соответствие профилям защиты информации.

Механизм обеспечения корня доверия

В современных микроконтроллерах для IoT-приложений большую роль играет обеспечение корня доверия на основе аппаратных механизмов, заложенных производителем. В СМК «Элиот» доверенная загрузка обеспечивается с использованием криптографических методов защиты и контроля целостности на основе ГОСТ Р 34.11-2012.

Поддержка криптографических алгоритмов

Международные криптографические стандарты поддерживаются блоком Arm Crypto Cell (блочные шифры AES, DES, аппаратная поддержка RSA и алгоритмов распределения ключа DH, вычисления контрольных сумм ECC, HASH и HMAC). Поддержка отечественных криптографических алгоритмов реализуется посредством ПО в составе модуля Aladdin Secure Firmware (от компании «Аладдин Р.Д.») с возможностью аппаратной акселерации ключевых операций. Программная реализация с аппаратной акселерацией обеспечивает уникальные скоростные характеристики криптографических вычислений (как при шифровании, так и вычислении хеш-функций) с учетом оптимизированных параметров площади кристалла и энергопотребления, что особенно важно для IoT-приложений.

Криптографическая библиотека обеспечивает следующие возможности:

- поддержку алгоритмов блочного шифрования «Кузнечик» (GHP) и «Магма» (MGM) в соответствии с ГОСТ Р 34.12-2015;
- обеспечение режимов ECB, CTR, OFB, CBC, CFB и вычисление имитовставки в соответствии с ГОСТ Р 34.13-2015 для алгоритмов «Кузнечик» и «Магма»;
- вычисление функции хеширования «Стрибог» (STBG) 256 и 512 бит в соответствии с ГОСТ Р 34.11-2012 с возможностью работы как независимо, так и параллельно с блочными вычислителями для шифруемых или дешифруемых данных;
- вычисление функции HMAC в соответствии с рекомендациями Р 50.1.113-2016.

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ СнК «ЭЛИОТ»

Программное обеспечение СнК «Элиот» состоит из инструментального ПО и системного ПО. ПО микросхемы позволяет проводить быструю разработку приложений для использования в промышленных устройствах Интернета вещей.

В состав инструментального ПО входят средства разработки и отладки программ, в том числе:

- инструментальное ПО для ядер общего назначения Arm Cortex-M33;
- стандартная библиотека языка C;
- стандартная библиотека языка C++;
- средства отладки программ JTAG, SWD;
- интегрированная среда разработки и отладки программ.

В состав средств разработки входит компилятор языка C/C++ для процессорных ядер Arm Cortex-M33. Компилятор основан на коде gcc с поддержкой всех стандартов.

Для отладки программного обеспечения используется отладчик GDB и openocd-сервер, предоставляющие возможность удаленной отладки ПО, работающего на модулях с СнК «Элиот» (рис. 2). Средства отладки обеспечивают выполнение команд отладчика GDB, GDB-сервера, Telnet-сервера openocd, возможность использования команд python через python-расширения GDB.

Все инструментальные средства доступны под интерфейсом единой интегрированной среды разработки и отладки разработки IDE MCStudio, реализованной на основе Eclipse (рис. 3).

Системное ПО СнК «Элиот» поддерживает жизненный цикл устройств на базе модулей, оснащенных этой микросхемой, интеграцию в сетевую инфраструктуру и инфраструктуру обновления ПО, обеспечивает исполнение требований по безопасности, предъявляемых к защищенным системам и комплексам.

В состав системного ПО входят следующие компоненты:

- доверенный начальный загрузчик;
- TF-M – среда исполнения Trusted Firmware-M;
- HAL (пакет поддержки процессора);
- операционная система реального времени Mbed OS.

Доверенный начальный загрузчик при включении питания обеспечивает загрузку образа операционной системы в память, проверку подписи загруженного образа и передачу управления загруженному коду.

Цепочка доверия обеспечивается за счет последовательной загрузки

Основные характеристики СнК «Элиот» (1892BM268):

- технология изготовления: КМОП, процесс 40 нм TSMC;
- рабочая частота ядер Arm Cortex-M33: 50 МГц (первое процессорное ядро CPU0), 160 МГц (второе процессорное ядро CPU1);
- три контура защиты, поддерживающие разделение ресурсов чипа на открытые и безопасные, и средства контроля целостности и подлинности встроенного программного обеспечения:
 - контур для начальной доверенной загрузки СнК;
 - контур защиты Arm TrustZone;
 - контур для поддержки международных и отечественных стандартов программной криптографии;
- встроенный блок цифрового навигационного контроллера: поддержка стандартов ГЛОНАСС/GPS;
- обеспечение режима пониженного энергопотребления: ток потребления в режиме Backup (RTC + 1 кбайт SRAM) до 10 мкА;
- напряжение питания:
 - основной источник питания: 2,5–3,6 В,
 - батарейный источник питания: 1,6–3,6 В,
 - три уровня напряжения питания ядра: 0,9/1,0/1,1 В,
 - встроенные DC/DC-преобразователи питания;
- температурный диапазон: –60...85 °С;
- тип корпуса: LFBGA132 (7×7 мм), шаг выводов 0,5 мм.

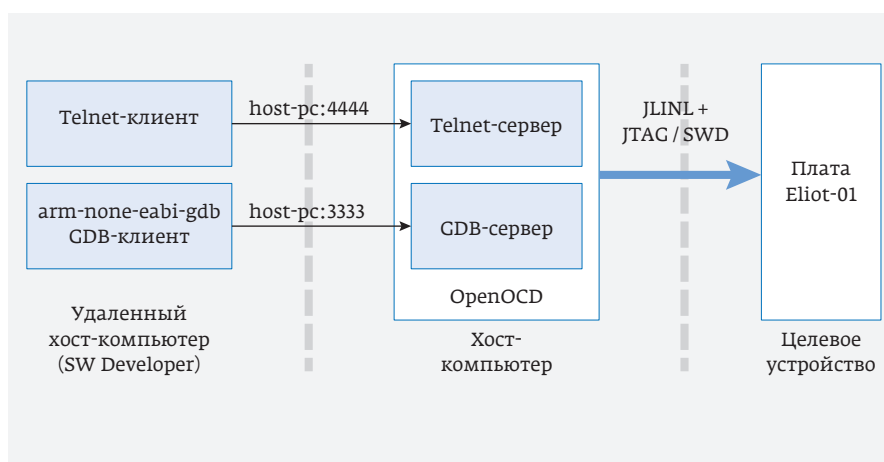


Рис. 2. Схема отладки ПО СнК «Элиот»

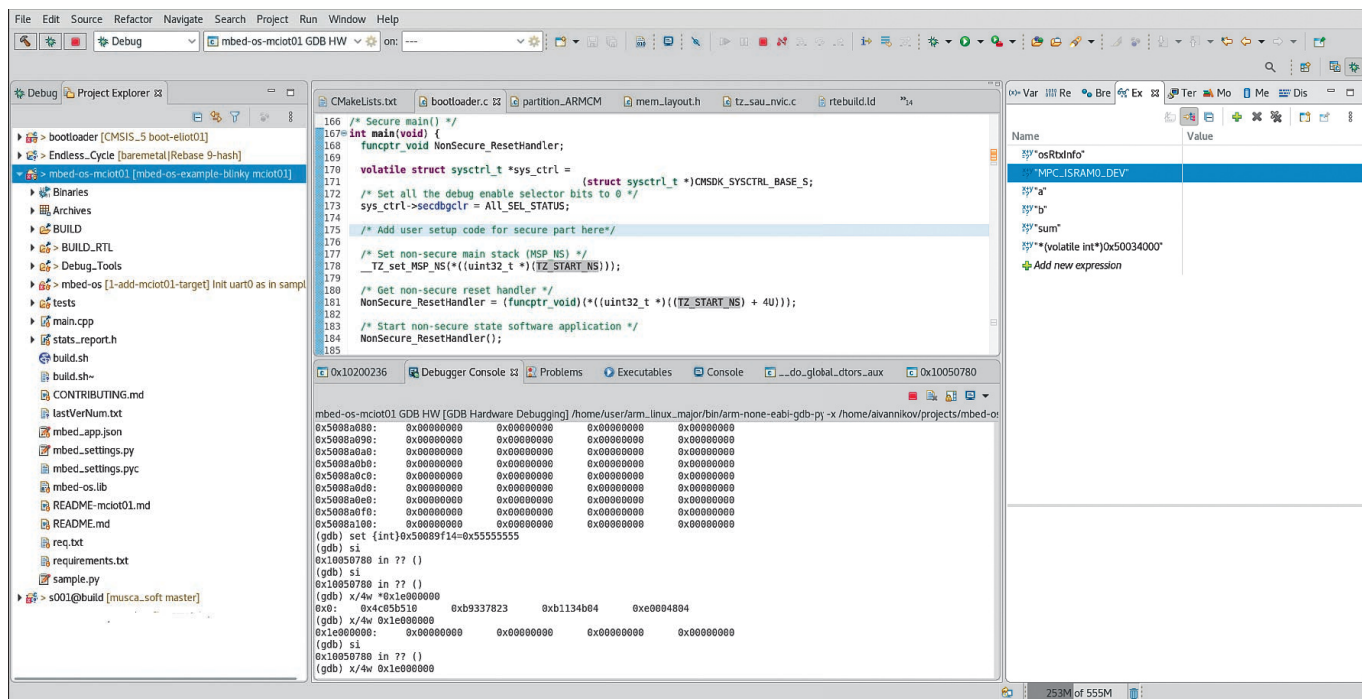


Рис. 3. Графический интерфейс IDE MCStudio

и проверки цепочки сертификатов. Доверенный начальный загрузчик удовлетворяет требованиям Arm Trusted Board Boot Requirements, предъявляемым к устройствам с аппаратным корнем доверия (Root-Of-Trust).

Trusted Firmware-M обеспечивает имплементацию ПО безопасной части устройств и микросхем на базе архитектуры ARMv8-M согласно требованиям стандарта PSA (Platform Security Architecture) с использованием аппаратных расширений TrustZone. TF-M поддерживает микросхемы с архитектурой CPU Cortex-M33, Cortex-23.

Системное ПО, использующее TF-M, состоит из следующих компонентов (рис. 4):

- TF-M (обозначено синим цветом на рис. 4). Разрабатывает вендор микросхемы и его технологический партнер, отвечающий за разработку доверенного системного ПО и СКЗИ;
- ПО, работающее в безопасном контуре микросхемы (обозначено зеленым цветом на рис. 4). Разрабатывает технологический партнер, отвечающий за разработку набора готового типового системного ПО или производитель устройства (прошивки);

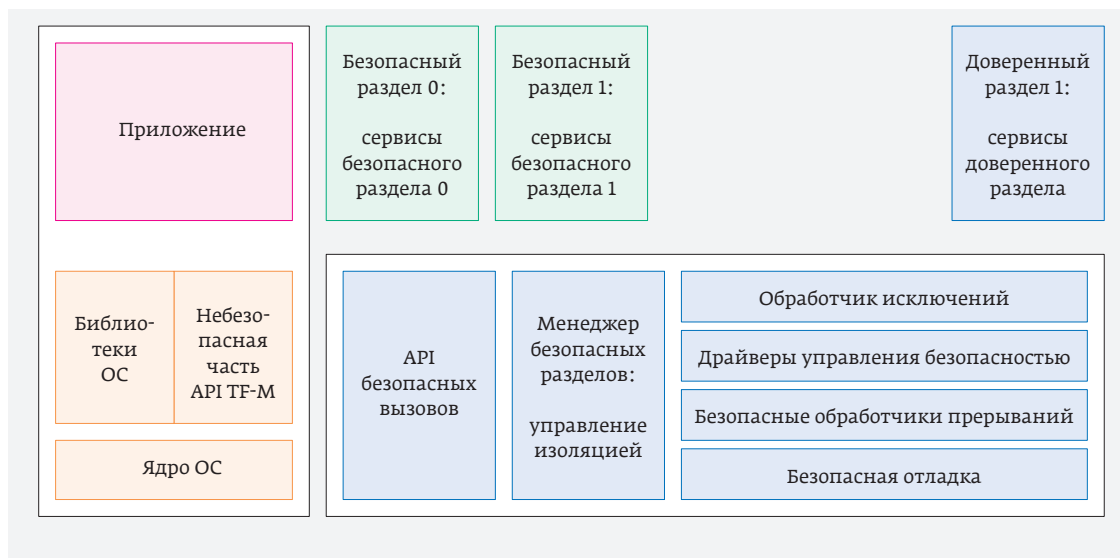


Рис. 4. Структура Trusted Firmware-M

- операционная система, работающая в небезопасном контуре микросхемы (обозначено желтым цветом на рис. 4). Разрабатывает вендор микросхемы, технологический партнер или производитель устройства (прошивки);
- приложение ОС, работающее в небезопасном контуре микросхемы (обозначено красным цветом на рис. 4). Разрабатывает производитель устройства (прошивки).

Trusted Firmware-M обеспечивает соблюдение требований PSA в части разделения ресурсов микросхемы (память, периферийные устройства) для использования в безопасном контуре и небезопасном контуре. Технология TrustZone разделяет используемую память и устройства на три области: NS (non-secure), S (secure), NSC (non-secure callable). С помощью TrustZone в системе выделяется ряд данных, функций и областей памяти, доступ к которым является критически важным и предоставляется только доверенной операционной системе (рис. 5).

Основной исполняемой ОС является гостевая ОС (Non-trusted firmware). В моменты, когда необходимо выполнить какие-либо критические функции или обратиться к критическим участкам памяти, гостевая ОС передает управление доверенной ОС (trusted secure firmware).

ОС небезопасного контура микросхемы во время работы может отсылать системные запросы в безопасный контур. В безопасном контуре отслеживание и обработка

системных запросов осуществляются TF-M, набором доверенных сервисов и функций.

Mbed OS – специализированная ОС для применения в IoT-устройствах. Она позволяет разделять между прикладными задачами пользователя аппаратные ресурсы целевого устройства (центральный процессор, оперативную память, порты ввода-вывода), а также осуществлять взаимодействие между задачами.

ОСРВ Mbed OS поддерживает:

- функциональность и API операционных систем реального времени;
- сетевые стеки, применяемые во встраиваемых устройствах;
- функции аппаратной безопасности (поддерживаются за счет использования гипервизора, управляющего аппаратными возможностями архитектуры Arm TrustZone, API взаимодействия с Trusted Firmware-M).

ПОЛЬЗОВАТЕЛЬСКАЯ ПРОГРАММНО-АППАРАТНАЯ ПЛАТФОРМА СнК «ЭЛИОТ» И ЕЕ ПРИМЕНЕНИЕ

АО НПЦ «ЭЛВИС» совместно с ЗАО «Аладдин Р. Д.» разрабатывает линейку модулей, предназначенную для разработчиков любого уровня, для создания широкого спектра устройств и обеспечивает быстрый вывод IoT-систем на рынок.

Базовым элементом линейки является модуль JC-4-Base (рис. 6) на базе СнК «Элиот». Данный модуль легко интегрируется в разрабатываемые с использованием СнК устройства. Предлагаемая линейка модулей обеспечивает реализацию навигационного приемника, а также расширение СнК модемами беспроводных и проводных интерфейсов. Применение готовых модулей может существенно сократить время разработки пользовательских устройств на базе СнК «Элиот».



Рис. 5. Разделение ресурсов в TrustZone

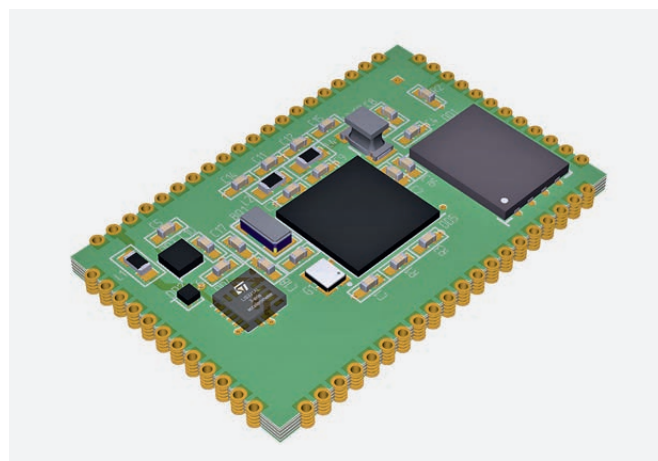


Рис. 6. Базовый модуль JC-4-Base

Отладочная аппаратно-программная платформа для СнК «Элиот» позволяет работать с набором модулей с целью разработки и отладки пользовательского программного обеспечения и обладает широким спектром интерфейсов.

Высокая безопасность, обусловленная архитектурой СнК «Элиот», позволяет эффективно применять ее для создания защищенных флеш-накопителей, обеспечивать безопасное локальное хранение данных и передачу данных на сервер и т. п.

Стек программного обеспечения пользовательской аппаратно-программной платформы СнК «Элиот» базируется на инструментальном ПО микросхемы и адаптирован для решения широкого круга задач потребителей.

Основными компонентами ПО являются:

- инструментальное ПО для ядер общего назначения ARM Cortex-M;
- интегрированная среда разработки и отладки программ;
- средства накристалльной отладки посредством JTAG;
- прикладные библиотеки для задач криптообработки и навигации;
- пакет поддержки процессора.

ЭКОСИСТЕМА СнК «ЭЛИОТ»

Востребованность и в целом успех СнК определяются не только ее характеристиками, но и экосистемой, создаваемой партнерами АО НПЦ «ЭЛВИС», среди которых дизайн-партнеры, сделавшие свой вклад на этапе проектирования СнК, разработчики прошивок, разработчики сервисного ПО (системы удаленного управления, доставки обновлений и профилирования микроконтроллеров, системы управления криптографическими ключами и СКЗИ), разработчики прикладного ПО, разработчики конечных устройств, а также потребители конечных устройств.

Существенный вклад в развитие экосистемы СнК «Элиот» внесла компания «Аладдин Р.Д.». Помимо реализованных механизмов безопасности (доверенный загрузчик Aladdin TSM-M, Aladdin Secure Firmware), компания ведет разработку комплекса системного, сервисного, прикладного ПО, системы централизованного управления жизненным циклом как самих микроконтроллеров, так и устройств на его основе, сертификатов и др. Все разрабатываемые компанией решения проходят сертификацию на соответствие требованиям по безопасности. Это позволит сильно облегчить задачу разработчикам прикладного ПО и конечных устройств.

АО НПЦ «ЭЛВИС» стремится к расширению сотрудничества и приветствует вступление в экосистему СнК «Элиот» новых партнеров для обогащения решений на ее основе.

ОБЛАСТИ ПРИМЕНЕНИЯ СнК «ЭЛИОТ»

Модули платформы на базе СнК «Элиот» могут применяться в таких сегментах рынка, как навигация (БПЛА, транспорт, трекеры), сбор данных с сенсоров и периферийных устройств (медицина и безопасность), безопасное локальное хранение, обработка и передача данных на сервер («умный дом», «умный город», «умные вещи»).

Среди ключевых приложений для СнК можно выделить:

- мониторинг параметров (мониторинг подвижных объектов, мониторинг параметров стационарных технологических объектов);
- контроль и управление устройствами (контроль местоположения технологических устройств, удаленное управление технологическими устройствами, трекинг и управление подвижными объектами);
- сбор, обработка, передача и хранение информации (сбор данных, предобработка; безопасное локальное хранение и обработка полученных данных; безопасная передача полученных данных на сервер по локальной сети/сетям общего пользования; построение локальных mesh-сетей; создание распределенных сетей; предобработка массивов параметров).

Микросхема найдет свое применение в промышленной автоматике (IIoT) и M2M в качестве компонента для умных устройств по сбору и обработке данных, модулей управления и контроля БПЛА, управления другими исполнительными устройствами.

ОТЕЧЕСТВЕННАЯ ТЕХНОЛОГИЧЕСКАЯ ПЛАТФОРМА УПРАВЛЕНИЯ ЖИЗНЕННЫМ ЦИКЛОМ СИСТЕМ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ НА ОСНОВЕ СнК «ЭЛИОТ», «СКИФ» И «РОБОДЕУС»

В АО «НПЦ «ЭЛВИС» разработаны три новые для российского рынка линейки микросхем, первыми представителями которых являются:

СнК «Рободеус» или RoboDeus (1892BM248) – 50-ядерная гетерогенная СнК для встраиваемых систем и робототехники [1]. Микросхема позволяет эффективно реализовать практически любой тип алгоритма (управление, обработка графики и сигналов, связь, решение навигационных задач, обработка и распознавание изображений и видео, распознавание звука и вычисление любых типов нейросетей). Все задачи можно решать в концепции fusion sensors, то есть обрабатывать информацию от всех типов датчиков одновременно для достижения синергетического результата.

СнК «Скиф» или Scythian (1892BA018) – 11-ядерная гетерогенная (СнК) для построения мобильных и встраиваемых интеллектуальных систем для связи, телекоммуникаций, навигации, мультимедиа, мультисенсорной

обработки сигналов, робототехнических систем, планшетов, smart-камер, систем мониторинга – везде, где требуется сложная обработка информации в условиях ограниченного энергопотребления и обеспечения доверенности [2].

СнК «Элиот» или Eliot (1892BM268) – малопотребляющая 2-ядерная СнК, которая, в первую очередь, предназначена для применения в качестве микроконтроллера для Интернета вещей и поддержки концепции «от периферии к облаку».

Комплект СнК «Элиот», «Скиф» и «Рободеус», разработанный АО НПЦ «ЭЛВИС» в рамках реализации государственной программы «Развитие электронной и радиоэлектронной промышленности», позволит эффективно решить проблему информационной безопасности и служить основой для создания отечественной технологической платформы управления жизненным циклом систем критической информационной инфраструктуры (КИИ). Среди областей применения следует назвать: ОПК, транспорт, информационно-телекоммуникационные сети, топливно-энергетический сектор, кредитно-финансовую сферу, промышленность (оборудование и системы для промышленной автоматизации, в частности IIoT), атомную отрасль, государственные организации и органы власти, системы и средства защиты информации, M2M-коммуникации и т. п.

Отечественная технологическая платформа обеспечит эффективное импортозамещение оборудования и ПО для предприятий КИИ, предотвратит утечки информации, перехват управления, блокирование работы, вывод из строя оборудования и инфраструктуры, протоколов обменов, ОС, СУБД, встроенного, системного и прикладного ПО, закладки для кражи данных и проведения удаленных компьютерных атак.

Успех отечественной технологической платформы основан, прежде всего, на том, что впервые, компанией «ЭЛВИС» вместе с партнерами были разработаны ЭКБ, ПО и новый подход к проектированию доверенных систем – Secure by Design – не после завершения разработки компонентов платформы, а в процессе одновременного и сквозного проектирования всех ее компонентов (ЭКБ, ПО). Важно, что проектирование СнК выполнено с участием ведущих российских компаний в области защиты информации (АО «Лаборатория Касперского», ЗАО «Аладдин Р. Д.» и др.).

Следует отметить, что СнК «Элиот» может использоваться, прежде всего, в IoT-приложениях, требующих высокой степени безопасности и доверия к конечному устройству, основанных на отечественной СКЗИ и технологии Arm TrustZone, а также на встроенном в СнК навигационном решении.

Устройства на основе СнК «Элиот» могут обеспечить:

- дистанционный мониторинг (сбор информации; мониторинг системы в режиме реального времени (сенсоры, датчики, камеры, БПЛА); оповещения о неисправности или опасности);
- управление активами в реальном времени (отслеживание точного расположения и технического состояния любого оборудования в реальном времени; анализ данных, принятие решений; выявление операционных или экологических опасностей, своевременное оповещение об этом ответственных лиц);
- профилактическое обслуживание оборудования, во время которого, благодаря датчикам, работающим с СнК «Элиот», отслеживаются такие характеристики, как температура хладагента, низкий уровень заряда батареи, перегрев двигателей, увеличение выброса загрязняющих веществ в окружающую среду и т. д. Данные эко-мониторинга могут использоваться для анализа состояния оборудования и принятия решений, а данные о состоянии оборудования – для прогнозирования экологической обстановки.

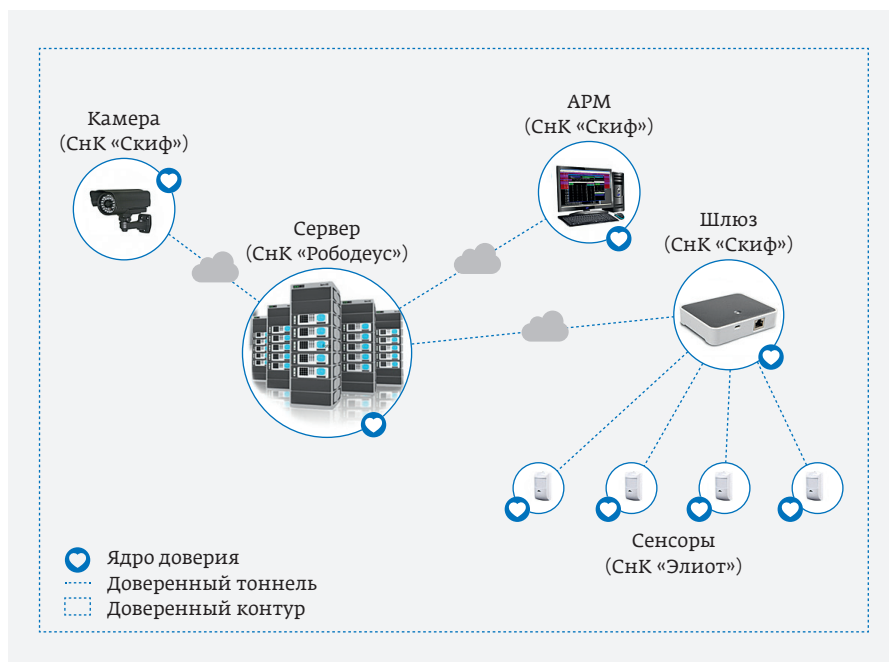


Рис. 7. Единая безопасная сквозная технологическая платформа эко-мониторинга на основе микросхем разработки АО НПЦ «ЭЛВИС» – СнК «Рободеус», СнК «Скиф» и СнК «Элиот»

На рис. 7 представлен пример реализации единой сквозной безопасной технологической платформы для систем экологического мониторинга на основе СМК «Рободеус» (серверное оборудование с ИИ), камеры, АРМ, шлюза на базе СМК «Скиф», IoT-сети на базе СМК «Элиот» и сенсоров. В системе обеспечены не только ядра и контуры доверия (на базе локальных ресурсов, используемых СМК), но и доверенные облачные тоннели.

IoT-платформы, реализуемые сегодня в рамках концепции «Индустрия 4.0», обеспечат прирост эффективности производства и сокращение затрат на техническое обслуживание, прогнозирование и предотвращение отказов оборудования, снижение эксплуатационных расходов, повышение энергоэффективности, увеличение производительности труда, экономический рост и конкурентоспособность предприятий [3]. Такие компании, как Microsoft, Amazon, Baidu, IBM, Alibaba и Cloudera, осуществили успешное развитие своих IoT-платформ по принципу «от облака к периферии». Объем создаваемых и анализируемых в IoT-сетях данных огромен, что требует применения технологий Big Data, моделирования процессов

и принятия решений с участием технологий искусственного интеллекта.

Технологии безопасности на базе представленной в статье отечественной ЭКБ обеспечат доверенность всех компонентов новой цифровой технологической платформы, повысят уровень информационной безопасности и эффективность промышленного производства в России.

ЛИТЕРАТУРА

1. **Петричкович Я. Я., Солохина Т. В., Кузнецов Д. А., Меньшенин Л. В., Беляев А. А. и др.** RoboDeus – 50-ядерная гетерогенная СМК для встраиваемых систем и робототехники // ЭЛЕКТРОНИКА: Наука, Технология, Бизнес. 2020. № 7. С. 52–63.
2. **Петричкович Я. Я., Солохина Т. В., Кузнецов Д. А., Меньшенин Л. В., Беляев А. А. и др.** «Скиф» – система на кристалле для мобильных и встраиваемых систем связи, навигации и мультимедиа // ЭЛЕКТРОНИКА: Наука, Технология, Бизнес. 2020. № 8. С. 120–129.
3. www.iotconf.ru