Cortex-M33 — новый стандарт безопасности для NB-IoT

Вадим ГИЗЯТУЛИН
Владимир АПАРИН

С каждым годом безопасность IoT-устройств становится все более актуальной. Компания Nordic Semiconductors первой на рынке выпустила NB-IoT модуль nRF9160 на базе ARM-овских ядер Cortex-M33 и CryptoCell-310. Разберем, какие возможности предоставляет разработчику использование этих ядер.

Модем nRF9160 (рис. 1) представляет собой систему в корпусе (SiP — system in package) с модемом LTE-NB/CatM и навигационным приемником. Решение поддерживает все частоты, используемые в сетях NB-IoT и CatM, поэтому нет необходимости обращаться к различным модификациям устройств для разных регионов. Энергоэффективный Cortex-M33 с 1 Мбайт Flash-памяти и 256 кбайт RAM предоставляет разработчикам широкие возможности для создания приложений.

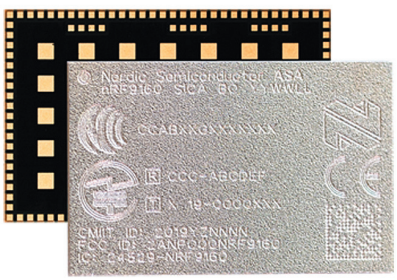

Рис. 1. Внешний вид модуля nRF9160

Технические характеристики nRF9160:

- LTE bands B1/2/3/4/5/8/12/13/14/17/18/19/20/25/26/28/66;
- 64 МГц ARM Cortex-M33;
- ARM TrustZone;
- ARM CryptoCell-310;
- 1 Мбайт Flash и 256 кбайт RAM;
- 4×SPI/UART/TWI PDM, I²S, PWM, АЦП;
- автоматизированное управление питанием и часами;
- 32 GPIOs.

Однако отличительной чертой nRF9160 является безопасность. Cortex-M33 оснащен модулями TrustZone для ARMv8-M, которые помогают защищать данные приложений и программное обеспечение, используя изолированную доверенную среду для ЦП и ОС.

Упрощая, можно сказать, что технология TrustZone позволяет разделить код и данные на две части: обычную, к которой привыкли все и широко используют, например в Cortex-M4, и защищенную, в которой исполняется код и хранятся данные, требующие защиты.

TrustZone в процессорах ARMv8-M (рис. 2) предлагает аппаратный контроль доступа к коду, памяти и вводу/выводу, сохраняя при этом требования встроенных приложений: отклик в реальном времени, минимальные накладные расходы на переключение, ограниченные ресурсы на кристалле и простоту разработки программного обеспечения. Технология TrustZone позволяет разделить систему и программное обеспечение на «безопасный» и «нормальный» миры. Безопасное программное обеспечение может получать доступ как к защищенным, так и к незащищенным ресурсам и памяти, тогда как обычное программное обеспечение может обращаться только к незащищенным ресурсам и памяти. Эти состояния безопасности ортогональны существующим режимам Thread и Handler, что позволяет использовать режимы Thread и Handler как в безопасном, так и в незащищенном состоянии.

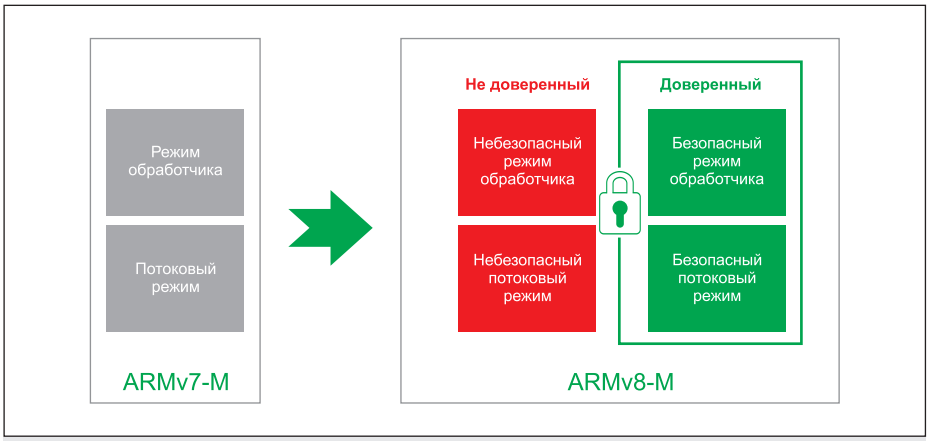

Рис. 2. TrustZone в процессорах ARMv8-M

Структура TrustZone включает следующие элементы:

- четыре стека и четыре регистра указателя стека;
- проверка аппаратного ограничения стека;
- программируемый блок защиты памяти, разделяющий пространство на безопасную и незащищенную области;
- система обработки исключений автоматически сохраняет и затем очищает безопасные состояния регистров при переключении в незащищенное состояние исключения;
- функция вызова незащищенного кода из защищенной области с контролем исполнения при помощи инструкций Secure Gateway (SG).

Прошивка может быть загружена в безопасную область для использования в системе незащищенными приложениями, будучи при этом полностью защищенной. Код супервизора, помещенный в безопасную область, может применяться для восстановления системы после программной атаки или ненадежной работы, в то время как незащищенная область остается доступной для разработчиков, которые в настоящее время создают програм-мное обеспечение для

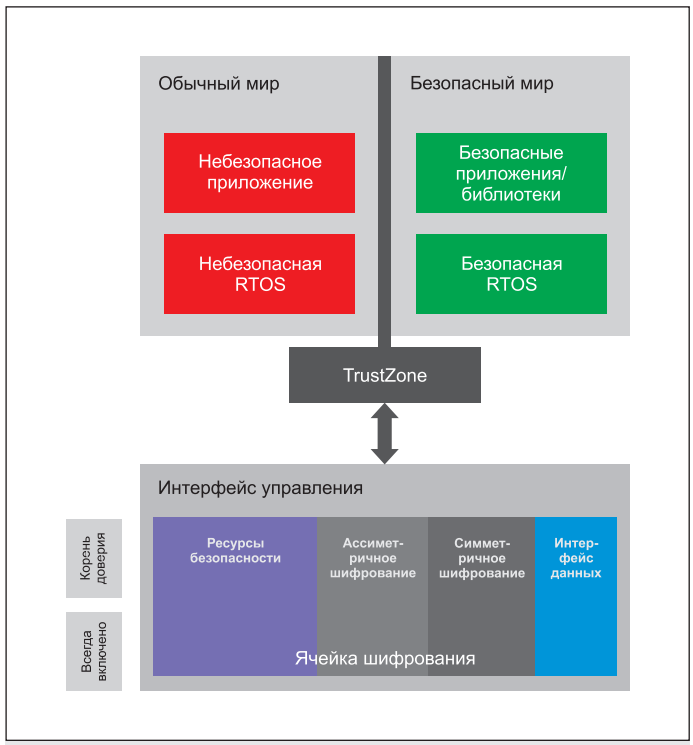

Рис. 3. Структура ARM TrustZone CryptoCell

Cortex-M. ARMv8-M добавляет дополнительное состояние к работе процессора, так что имеются как безопасные, так и небезопасные состояния выполнения.

Как уже упоминалось, технология TrustZone условно разделяет микроконтроллер на два мира — нормальный и безопасный. Это позволяет перенести обработку конфиденциальной информации в изолированную защищенную среду. CryptoCell — расширение ARM TrustZone, реализующее дополнительные функции аппаратно, а именно хранилище ключей, ускорители шифрования, генератор случайных чисел, блоки проверки кода, ключей и безопасной отладки. CryptoCell дополняет TrustZone и повышает безопасность устройства (рис. 3), при этом не снижая производительности устройства, так как используются аппаратные ускорители. TrustZone предлагает аппаратное управление доступом к коду, памяти и интерфейсам ввода/вывода данных, позволяя работать в обычных условиях встроенных приложений: отклик в реальном времени, минимальные задержки на коммутацию, ограниченные ресурсы на кристалле и простота разработки программного обеспечения.

Компания ARM представила свою технологию Platform Security Architecture (PSA) на основе ядер CryptoCell и Cortex-M33 еще в 2017 году (рис. 4), но реальные серийные микросхемы появились лишь в конце 2018 — начале 2019 года.

PSA предназначена для защиты недорогих IoT-устройств, в которых невозможно обеспечить доверительную среду (TEE, Trusted Execution Environment). Идея PSA заключается в том, чтобы отделить критичные части системы (ключи, права, учетные данные, прошивку) от аппаратных и программных компонентов, подверженных взлому. PSA определяет безопасную среду Secure Processing Environment (SPE) для этих

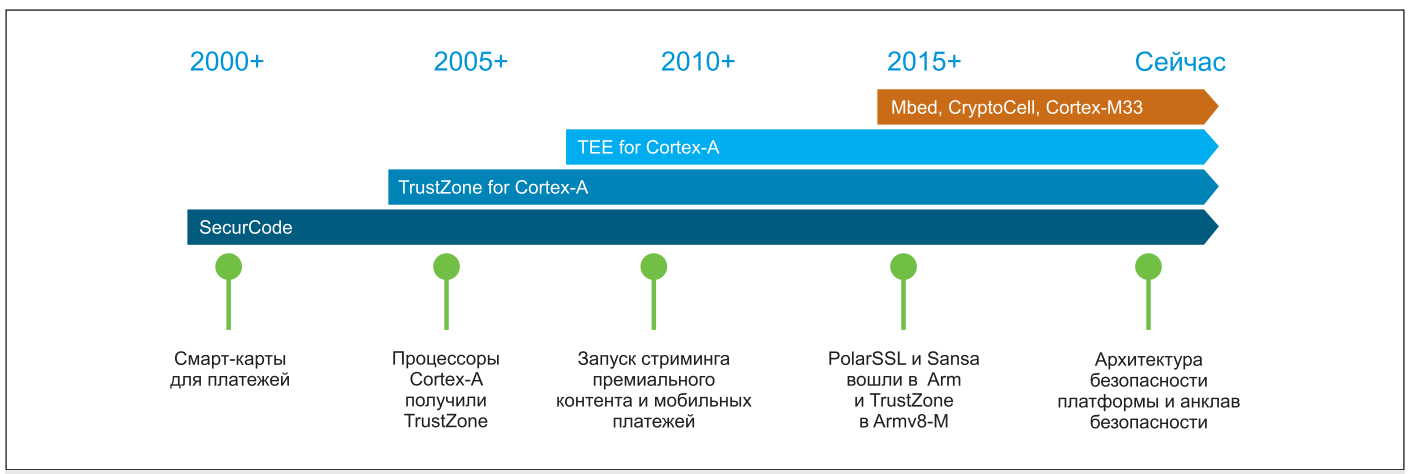

Рис. 4. Развитие ARM в сфере платформ безопасности

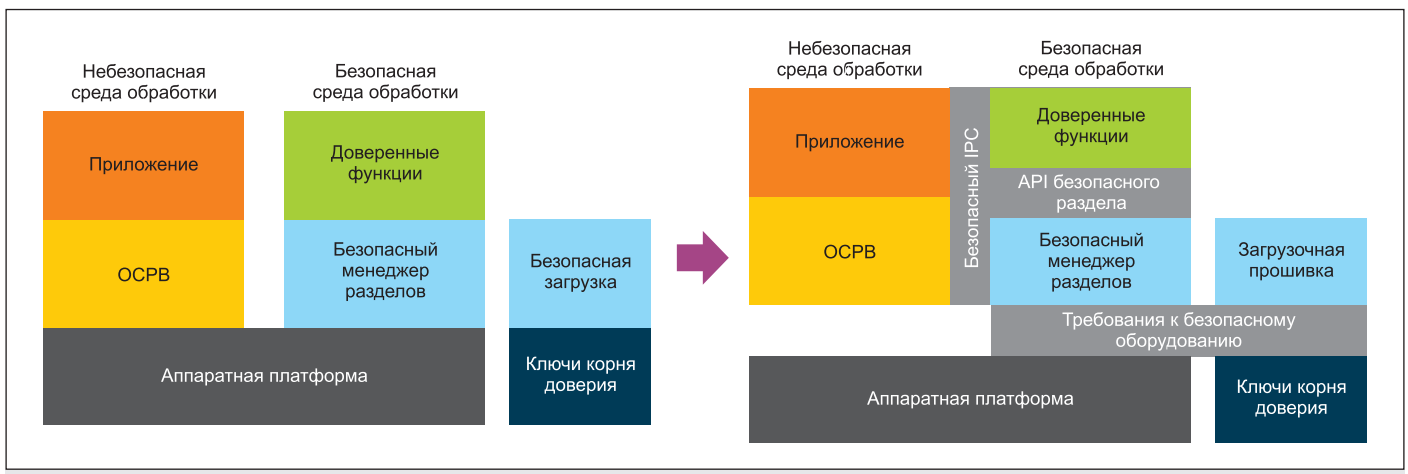

Рис. 5. Архитектура PSA

данных, код, который управляет ими, и надежные аппаратные ресурсы (рис. 5). Технология ориентирована в первую очередь на Cortex-M, но совместима со всеми семействами Cortex-A/-R/-M.

ARM TrustZone Cryptocell в Cortex-M33 обеспечивает безопасное хранение ключей (в том числе с уникальным аппаратным идентификатором), проверку прошивок (например, при обновлении по воздуху), генераторы случайных чисел (TRNG, PRNG), аппаратное ускорение шифрования AES, SHA, ChaCha, ECC, в том числе с DMA. То есть все данные во Flash и RAM могут быть зашифрованы. Следует отметить, что CryptoCell позволяет иметь несколько корней доверия для различных задач, а также безопасную отладку (Secure Debug) с авторизацией прав.

Трехсотая серия CryptoCell ориентирована именно на малопотребляющие IoT-устройства. Потребление новых M33 примерно на 20–40% ниже, чем M4, учитывая потери в энергопотреблении на работу TrustZone, в 20% имеем такой же или более низкий уровень потребления, чем сейчас. То есть аппаратная безопасность пришла в наиболее массовый бюджетный сегмент с Cortex-M33 и в ближайшее время количество продуктов на их базе будет только увеличиваться.

Ранее TrustZone был доступен только для производительных семейств Cortex-A, однако за последний год многие производители беспроводных систем выпустили свои решения на базе Cortex-M и в перспективе планируют переход на Cortex-M33.

В апреле 2020 года Cortex-M33 были сертифицированы по уровню EAL6+ по системе общих критериев (Common Criteria) информационной безопасности. Это очень высокий уровень безопасности, который позволяет использовать эти решения в высокорисковых ситуациях. Для сравнения, уровень EAL5 имеют смарт-карты (банковские, транспортные, в том числе бесконтактные), уровень EAL4 или EAL4+ у большинства операционных систем Windows и Linux.

Подводя итоги, нужно подчеркнуть, что модули Nb-IoT и LTE Cat-M являются переходным классом между 4- и 5-м поколением систем сотовой связи, ориентированных на низкопотребляющие сети LPWAN. В большинстве случаев устройства должны работать годами без вмешательства человека. Современные решения позволяют работать 7–10 лет на одном элементе питания (батарейке). Средний срок службы устройства часто достигает 15 лет. За это время могут значительно измениться требования по безопасности, появиться новые угрозы. Устройства при этом должны работать стабильно без вмешательства человека весь срок службы. Соответственно, необходимо защищать IoT-устройства с учетом срока и характера их работы.

Литература

1. **www.developer.arm.com/** статьи из раздела ARM TrustZone technology
2. **www.arm.com/products/silicon-ip-cpu/cortex-m/cortex-m33**
3. Arm Cortex-M33 Processor Datasheet.
4. Introducing ARM Cortex-M23 and Cortex-M33 Processors with TrustZone for ARMv8-M.
5. **www.developer.arm.com/** статья TrustZone CryptoCell-312 Security IP