ЭФФЕКТИВНОЕ РЕШЕНИЕ ВОПРОСОВ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ВО ВСТРАИВАЕМЫХ СИСТЕМАХ ИНТЕРНЕТА ВЕЩЕЙ

ПО МАТЕРИАЛАМ КОМПАНИИ RENESAS

Обеспечение безопасности встраиваемых систем интернета вещей может оказаться достаточно сложной и трудоемкой задачей даже для опытных разработчиков. Мы рассмотрим несколько наиболее часто возникающих вопросов проектирования этих систем и ознакомимся с решениями компании Renesas по безопасности на основе платформ, в которых используются все преимущества последних достижений в сферах аппаратного и программного обеспечения. Эти решения позволяют реализовать всестороннюю защиту на нескольких уровнях.

ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ УСТРОЙСТВ В ИНТЕРНЕТЕ ВЕЩЕЙ

К концу 2020 г. количество устройств интернета вещей составит около 31 млрд ед. Многие из них недостаточно хорошо защищены, что делает их легкой добычей для хакеров. В значительной степени многие встраиваемые системы уязвимы, потому что их защита – сложная задача. Разработчики должны хорошо разбираться в быстро меняющейся картине угроз, а также учитывать требования постоянно совершенствующихся стандартов безопасности. Бывает, в случае проектирования сложных приложений необходимо выполнить требования нескольких стандартов, что усложняет работу над обеспечением совместимости и функциональной гибкости устройств. Во многих случаях создание защиты более высокого уровня сопровождается увеличением финансовых расходов и энергопотребления, что отрицательно влияет на конкурентоспособность конечных устройств.

Мы рассмотрим несколько наиболее распространенных вопросов, возникающих при разработке встраиваемых систем, а также предоставим рекомендации, которые помогут повысить безопасность устройств, ускорить вывод на рынок изделий, сервисов и систем.

Итак, к наиболее распространенным вопросам по обеспечению безопасности встраиваемых систем относятся следующие:

1. Как защитить проектируемое устройство?
2. Как предотвратить появление на рынке несанкционированных копий устройств?
3. Как упростить управление безопасностью?
4. Как защитить идентификационную информацию об устройстве?
5. Что делать тем разработчикам, которые не являются экспертами в области обеспечения безопасности изделий?
6. Как обеспечить соответствие стандартам, получить техподдержку от поставщиков и реализовать конкурентоспособный проект?

ВОПРОС 1: КАК ЗАЩИТИТЬ ПРОЕКТИРУЕМОЕ УСТРОЙСТВО?

Несколько лет тому назад разработчикам приложений не приходилось волноваться о том, как обеспечить безопасность своих изделий, поскольку устройства и приложения не были настолько тесно связаны друг с другом так, как теперь. В настоящее время даже самые простые электронные устройства, начиная со светодиодных ламп и заканчивая радионянями и контейнерами с рецептурными препаратами, подключены к интернету или облаку. Слишком часто вопросы безопасности игнорируются или решаются, когда становится уже слишком поздно.

В текущем году защита данных и функциональных возможностей приложений интернета вещей от киберугроз является очень острой проблемой для разработчиков. Устройства необходимо оснащать функциями безопасности на этапе проектирования и на аппаратном, и на программном уровнях. Платформенный метод предусматривает несколько уровней защиты за счет использования последних достижений в аппаратном и программном обеспечении.

К эффективным аппаратным средствам обеспечения безопасности относятся следующие.

- Устройство должно безопасно генерировать и хранить ключи (в т. ч. закрытые ключи), чтобы исключить подмену и несанкционированный доступ к настройке устройства.
- Аппаратно ускоренное шифрование, хеширование и генерация истинно случайных чисел, благодаря чему ускоряются криптографические операции в устройстве. Такая аппаратная поддержка экономит время и энергопотребление.
- Защищенный доступ к памяти для защиты определенных областей ОЗУ и флэш-памяти от несанкционированного доступа. Отдельные области памяти изолируют конфиденциальный код и данные от небезопасного кода и данных; при этом память с однократной записью защищает код и данные от внесения изменений или перепрограммирования.
- Защищенный доступ к программированию и отладке, который снижает риски использования хакерами интерфейсов отладчика и программатора для атак.

К программным средствам относятся следующие.

- Интегрированное и оптимизированное ПО с проверенными средами разработки приложений и стандартными API-интерфейсами.
- API уровня драйверов для взаимодействия с аппаратными средствами безопасности.
- Криптографические библиотеки с набором API-интерфейсов, которые обеспечивают широкий ряд средств

безопасности, включая функции безопасности макроуровня, корень доверия (root-of-trust), а также способность распознавать доверенные источники и код.

– Встроенная поддержка стандартных протоколов связи и средств передачи данных, например протокол защищенной передачи гипертекстовой информации (HTTPS), безопасность на транспортном уровне (TLS) и прочие специальные облачные протоколы.

Компания Renesas уже много лет является лидером в области встраиваемых средств защиты информации и хорошо зарекомендовала себя в сфере безопасности современных подключаемых устройств. Компания Renesas предлагает платформенную методику для обеспечения безопасности встраиваемых систем. Эта методика предусматривает многоуровневую инфраструктуру разработки, которая гарантирует всестороннюю защиту широкого ряда встраиваемой продукции.

Renesas Synergy представляет собой комплексную профессиональную платформу для разработки, в состав которой входит программное обеспечение производственного уровня и масштабируемое семейство совместимых по выводам микроконтроллеров, интегрирующих протестированные аппаратные средства защиты на нескольких уровнях. Платформа Synergy гарантирует разработку приложений интернета вещей на основе безопасной и надежной технологии.

Synergy предоставляет несколько вариантов генерации ключей с помощью модуля Secure Crypto Engine (SCE) (см. рис. 1). Модуль SCE генерирует уникальную криптографическую аппаратную идентификационную информацию об устройстве, которая безопасно хранится во внутренней флэш-памяти благодаря безопасному блоку защиты памяти (SMPU) и окнам доступа к флэш-памяти (FAW). Эти средства защиты памяти, которыми оснащены микроконтроллеры Synergy, используются также для хранения кода защищенной загрузки, сертификатов и ключей наряду с другими конфиденциальными данными. Кроме того, модуль SCE хранит ключи в безопасности во избежание раскрытия конфиденциальной информации даже в небезопасной памяти. Изоляция ключей достигается с помощью симметричного шифрования ключей, уникальных для микроконтроллера; поскольку оно выполняется отдельно для каждого микроконтроллера, доступ к ключам осуществляется только внутри модуля SCE того микроконтроллера, который выполнил симметричное шифрование.

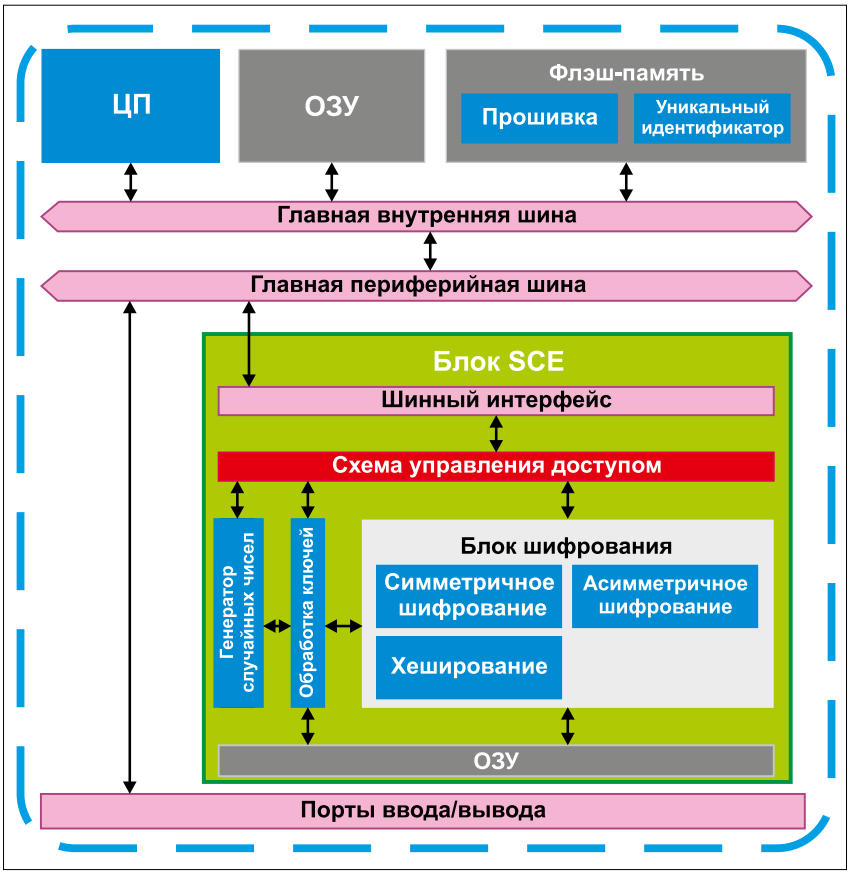

Рис. 1. **Изолированная подсистема Secure Crypto Engine в МК**

Платформа также должна устанавливать безопасное и простое соединение с облаком. По мере усложнения приложений интернета вещей и ужесточения требований к безопасности растет потребность в увеличении вычислительной мощности для обработки данных. Подключения к облаку должны быть безопасными, т. к. данные системы все больше зависят от облачных ресурсов с гипермасштабируемой инфраструктурой вычислений и хранения данных интернета вещей. Микроконтроллеры Synergy обеспечивают подключение к облаку с помощью встроенных модулей MQTT и TLS, а приложения Synergy предоставляют безопасное соединение с ведущими облачными средами, включая вебсервисы Amazon (AWS), облако Google Cloud и Microsoft Azure.

ВОПРОС 2: КАК ПРЕДОТВРАТИТЬ ПОЯВЛЕНИЕ НА РЫНКЕ НЕСАНКЦИОНИРОВАННЫХ КОПИЙ УСТРОЙСТВ?

Во избежание несанкционированного клонирования разработанных компанией изделий необходимо оснастить их фирменными функциями. В настоящее время глобальные цепочки поставок требуют более внимательного отношения и усиленной безопасности для поддержания целостности, а также аутентичности продукции на этапе создания и производства. Чтобы добиться этого, следует организовать безопасное производство, уменьшив риск кражи интеллектуальной собственности и сохранив целостность производственных процессов. Менеджер защищенной загрузки Synergy предоставляет решение, позволяющее надежно и безопасно встроить авторизованное ПО во флэш-память микроконтроллеров Synergy на удаленных производственных площадках (см. рис. 2). В результате встроенное ПО получает защиту от незаконного копирования, внесения изменений или его установки на скопированное аппаратное обеспечение.

Менеджер защищенной загрузки Synergy также обеспечивает надежный доверительный механизм, который предоставляет уникальную идентификационную информацию, аппаратно-защищенные ключи, безопасную программу начальной загрузки, безопасный модуль обновления флэш-памяти и криптографические API для взаимодействия с аппаратным обеспечением микроконтроллеров.

Код доверительного механизма предварительно загружается в устройства по защищенному соединению на этапе массового производства. Сконфигурированный кристалл хранит данные в изолированной области и осуществляют тщательный контроль доступа к этим данным.

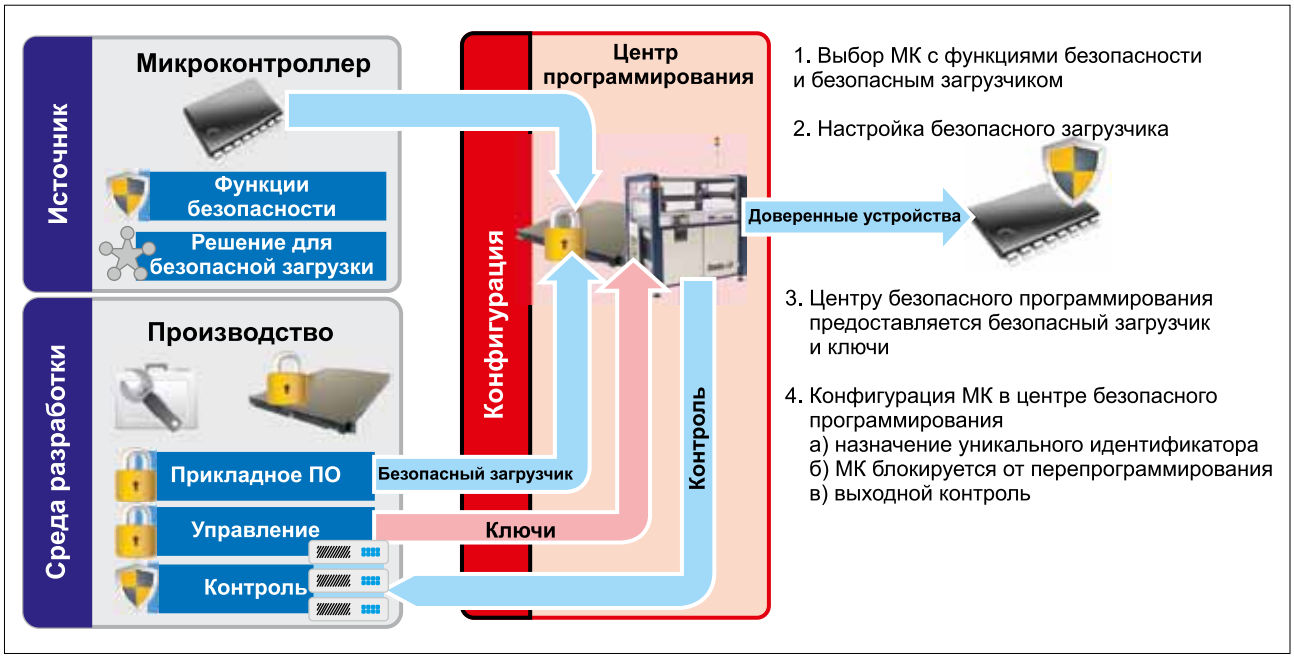

Рис. 2. **Renesas Synergy Secure Boot Manager – безопасное запатентованное решение для программирования флэш-памяти**

После ввода изделий в эксплуатацию менеджер защищенной загрузки может при необходимости безопасно обновить авторизованное встроенное ПО во флэш-памяти МК Synergy с помощью встроенного в кристалл доверительного механизма (root-of-trust), выполняющего проверку достоверности и дешифровку микропрограммы до ее записи во флэш-память. Программирование осуществляется с помощью безопасной облачной инфраструктуры, ставшей еще надежнее благодаря решениям компании Renesas для облачных подключений.

ВОПРОС 3: КАК УПРОСТИТЬ УПРАВЛЕНИЕ БЕЗОПАСНОСТЬЮ?

Проектирование всесторонней многоуровневой защиты для встраиваемых систем может оказаться трудоемкой задачей. Один из способов уменьшения расходов заключается в использовании в платформе разработки самых последних достижений и протоколов безопасности. Благодаря платформе Synergy разработчику нет надобности изучать новые и актуальные протоколы, а также прочие средства обеспечения безопасности для создания защищенного приложения.

Пакет прикладных программ Synergy упрощает реализацию сложных функций, применяемых для разработки подключаемых встраиваемых систем. Это программное обеспечение защищает области памяти, в которых создаются и хранятся части кода, защищенные от считывания и записи во флэш-память и статическое ЗУ с произвольной выборкой (SRAM). Благодаря этому можно создавать настраиваемые области памяти для хранения временных и секретных ключей, прочих конфиденциальных данных.

Платформа Synergy поддерживает инфраструктуру открытых ключей (PKI) – криптографическую методологию, которая обеспечивает аутентификацию с помощью цифровых сертификатов, а также предоставляет общий ключ (PSK) – модель шифрования, при которой оба одноранговых узла в цифровом соединении определяют один и тот же ключ. PSK-ключ осуществляет упрощенное шифрование и защиту на соответствующих уровнях, например используется для контроля доступа небольшого числа пользователей. Несмотря на более сложную инициализацию и управление, ключ PKI является формой ассиметричного шифрования, которое позволяет аутентифицировать пользователей, создавать и распределять сертификаты, а также поддерживать сертификаты, управлять и отзывать их. PKI-инфраструктура с открытыми и закрытыми ключами, которая считается более безопасной моделью шифрования, применяется для аутентификации в больших системах шифрования.

Платформа Synergy предоставляет оптимизированное коммерческое ПО со стандартными API, упрощающими создание интерфейсов с аппаратной защитой и средствами безопасности. Среды разработки приложений помогают устранить сложности интеграции беспроводных драйверов с помощью однородного интерфейса между кодом приложения и драйверами нижнего уровня. Такой уровень абстракции упрощает интеграцию сетевых стеков, удаление или добавление драйверов при необходимости.

ВОПРОС 4: КАК ЗАЩИТИТЬ ИДЕНТИФИКАЦИОННУЮ ИНФОРМАЦИЮ ОБ УСТРОЙСТВЕ?

Для защиты устройства от злоумышленников необходима защита идентификационной информации об устройстве путем генерации аппаратного ключа. Ее можно безопасно хранить во внутренней флэш-памяти, эффективно использовать для формирования доверительного доступа и обеспечения конфиденциальности при добавлении в системы и настройке целевых приложений.

Формирование достоверной идентификационной информации об устройстве позволяет идентифицировать и аутентифицировать каждое устройство интернета вещей как уникальное. Благодаря этому появляется возможность защитить каждое устройство по отдельности, установить зашифрованную связь с другими защищенными устройствами и службами. Достоверная идентификационная информация об устройстве обеспечивает многоуровневую защиту интернета вещей от угроз безопасности за счет следующих характеристик.

– *Доверие*. После подключения к сети устройство должно пройти проверку подлинности для формирования доверия между другими устройствами, службами и пользователями так, чтобы оно могло безопасно обмениваться зашифрованными данными и информацией. Доверие начинается с аутентификации устройства для

подтверждения того, что оно является настоящим, а не подделкой.

– *Конфиденциальность*. Данные и информация, собираемые и передаваемые внутри интернета вещей, часто включают в себя конфиденциальные, личные или финансовые данные, которые должны храниться в тайне и быть защищены в соответствии с нормативными требованиями. Защищенная идентификационная информация об устройстве формирует основу для обеспечения конфиденциальности, когда устройства интернета вещей и системы устанавливают связь для обмена данными.
– *Сохранность (целостность)*. Гарантия того, что данные, передаваемые внутри сетей, не были изменены, является ключевым элементом многоуровневой защиты. Сохранность данных – часто упускаемое из виду требование, но безопасность соединенных устройств и систем основана именно на подлинности (достоверности), конфиденциальности и сохранности передаваемой информации.

Защита цифровых данных также имеет высший приоритет для предотвращения угроз нарушения безопасности. Хранимые данные не передаются между устройствами или сетями – они обычно находятся в СОЗУ или энергонезависимом запоминающем устройстве. Для защиты хранимых данных микроконтроллеры Synergy оснащены средствами контроля доступа, включая защиту от считывания, записи, чтения/записи, однократной записи (см. табл.). Контроль доступа к хранимым данным уменьшает возможности атаки и повышает безопасность системы.

Кроме того, микроконтроллеры Synergy можно удаленно обновлять на месте эксплуатации для обеспечения защиты от новых киберугроз.

ВОПРОС 5: ЧТО ДЕЛАТЬ ТЕМ РАЗРАБОТЧИКАМ, КОТОРЫЕ НЕ ЯВЛЯЮТСЯ ЭКСПЕРТАМИ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИЗДЕЛИЙ?

Для обеспечения всесторонней защиты приложений со встроенными устройствами требуется высокоинтегрированная оптимизированная платформа, поддерживающая многие протоколы и средства защиты, которые работают совместно для обеспечения безопасности на нескольких уровнях.

Платформа Renesas Synergy предоставляет комплексную среду разработки с уникальным набором аппаратных и программных средств обеспечения безопасности. Они основаны на общем доверительном механизме, который отвечает требованиям к защите встраиваемых устройств и интернета вещей. Платформа также расширяет возможности безопасного масштабируемого производства и защиты интеллектуальной собственности.

Кроме того, разработчики также могут воспользоваться онлайн-библиотеками проектов приложений от Renesas для получения поэтапных инструкций и руководств по реализации решений со сквозной безопасностью.

Кроме того, проекты, выполненные на платформе Synergy, получают поддержку со стороны большого сообщества Renesas и экосистемы ассоциированных партнеров. Сеть обученных и сертифицированных партнеров по проектному обслуживанию Renesas предоставляет поддержку на каждом этапе проектирования. Эффективная помощь партнеров Renesas позволяет ускорить процесс разработки, расширить и углубить знания в области проектирования решений по безопасности.

ВОПРОС 6. КАК ОБЕСПЕЧИТЬ СООТВЕТСТВИЕ СТАНДАРТАМ, ПОЛУЧИТЬ ТЕХПОДДЕРЖКУ ОТ ПОСТАВЩИКОВ И РЕАЛИЗОВАТЬ КОНКУРЕНТОСПОСОБНЫЙ ПРОЕКТ?

Перед началом разработки следует выбрать подходящее решение по микроконтроллерам, которое обеспечивает высокоинтегрированную платформу с функциями, гарантирующими безопас-

Таблица. **Аппаратные средства защиты SCE микроконтроллеров Renesas Synergy по сериям**

		Функции	Упаковка ключей	NIST CAVP	S7	S5	S3	S1
Идентичность и обмен ключами (ассиметр.)	RSA	Генерация ключей, подпись/проверка[1]	Y	Y[5]	1024/2048/4096	1024/2048/4096		
	ECC[4]	Генерация ключей, ECDSA, ECDH[2]	Y	WIP	NIST P192/P224/ P256/P384	NIST P192/P224/ P256/P384		
	DSA	Подпись/проверка			L.2048/1024, N.256/226/160	L.2048/1024, N.256/226/160		
Конфиденциальность (симметр.)	AES	ECB, CBC, CTR	Y	Y	128/192/256	128/192/256	128/256	128/256
		GCM		Y	128/192/256	128/192/256	128/256	
		XTS, CCM			128/256	128/256	128/256	
	3DES	ECB			192	192		
		CBC			192	192		
		CTR			192	192		
Целостность данных	Хэш	GHASH		Y	Y	Y	Y	
		SHA1/224/256		Y	Y	Y		
	TRNG	Аппаратная среда с DRBG-AES-128		Y	Y	Y	Y	Y
	Уникальный ID				Y	Y	Y	Y
Защита данных	MPU	Arm, контроллер шины, исполнитель шины			Y	Y	Y	Y
	MPU	Безопасность				Y	Y	Y[3]
	FAW	Защита от программирования/стирания			Y	Y	Y	Y
	SCE	Криптомодуль			SCE7	SCE7	SCE5	
	SCE	Установка и упаковка ключей			Y	Y	Y	

[1] 4096-бит верификация, только шифрование.
[2] Через скалярное умножение.
[3] Недоступно для S124.
[4] Для драйверов низкого уровня требуется SSP v1.5.0.
[5] Для драйверов низкого уровня требуется SSP v1.6.0.

КОММЕНТАРИЙ СПЕЦИАЛИСТА

Андрей Лебедев, руководитель направления полупроводников, ООО «Сканти»

Обеспечение безопасности устройств с подключением к интернету – комплексная задача. Не за горами появление национальных стандартов безопасности и законов об интернете вещей. Вероятно, будет создан и единый регламент, предписывающий всем производителям устройств применять шифрование с определенной схемой обмена ключами установленной длины по какому-то одному протоколу.

Если конечное устройство подключено к любой открытой сети, обменивается данными или обновляется через сеть, необходима защита от взлома, перехвата и подмены данных. Необходимо в самом начале проектирования заложить «кирпичики» защиты устройств.

Компания Renesas предлагает мощный инструментарий – изолированные блоки флэш-памяти и ОЗУ, аппаратное шифрование в независимых блоках Trusted Secure IP и Secure Crypto Engine, защищенный уникальный номер кристалла и генератор случайных чисел.

Кроме того, Renesas использует схему Arm TrustZone в своих микроконтроллерах на ядрах Arm Cortex-M и Cortex-A. Компания получила сертификат PSA Certified level one от Arm и участвует в сообществах Trusted Firmware M и Trusted Firmware A для развития программно-аппаратных средств защиты IoT-устройств.

ность и защиту на нескольких уровнях. Злоумышленники могут воспользоваться уязвимостями во встраиваемых системах, если различия в протоколах проектирования и безопасности имеют слабые места. Эти различия особенно опасны, когда аппаратное обеспечение, ПО микроконтроллера, коммуникационные стеки и драйверы не стандартизованы в полностью интегрированной структуре.

Комплексная, полностью интегрированная платформа разработки обеспечивает максимально простую защиту проектов. Необходимо выбрать интегрированную среду, которая предварительно объединена с ключевым программным обеспечением, функциональными возможностями, стеками и драйверами, уже имеющимися в платформе. Такой выбор освобождает от необходимости работать с нижними уровнями интеграции, позволяя сосредоточить усилия на тех сторонах проекта, которые создадут конкурентные преимущества конечного изделия.

Кроме того, следует убедиться, что у выбранного поставщика решений имеется активная и комплексная партнерская экосистема. Возможность аутсорсинга для разработки определенных средств защиты или функций доверенными специалистами сэкономит время и повысит качество продукции.

Renesas Synergy – комплексная профессиональная платформа разработки, которая включает в себя ПО производственного уровня, масштабируемое семейство совместимых по выводам микроконтроллеров, среды разработки приложений, функциональные библиотеки, драйверы HAL (абстрактный аппаратный уровень), расширенные программные инструменты и пакеты. Она обеспечивает разработку приложений для интернета вещей на основе безопасной и надежной технологии. Благодаря встроенной многоуровневой защите каждое устройство можно идентифицировать и аутентифицировать уникальным образом для защищенной связи с другими устройствами, службами и пользователями.

Платформа оснащена функциями безопасности от Renesas, позволяя разработчикам в большей мере заниматься решениями задач более высокого уровня, которые соответствуют быстро меняющимся возможностям рынка интернета вещей и отвечают текущему спросу. Благодаря предварительной интеграции, тестированию и высокой квалификации инженеров компании Renesas можно начать разработку прикладного ПО на уровне API, сэкономив немало времени, отведенного на проектирование.

Разработчики также могут рассчитывать на опытных партнеров Renesas, которые готовы оказать помощь при разработке определенных средств или функций защиты, оказать поддержку или поделиться ценными навыками.

Компания Renesas помогает разработчикам встраиваемых систем решить задачи проектирования средств безопасности, предлагая платформенную методику на основе последних достижений в области аппаратной и программной безопасности. Платформа Renesas Synergy основана на общем доверительном механизме защиты устройств, служб и интернета вещей на глубоком уровне для обеспечения безопасного и масштабируемого производства, а также защиты интеллектуальной собственности на протяжении всего жизненного цикла изделий.

ЛИТЕРАТУРА

1. www.renesas.com/eu/en/doc/whitepapers/iot-security/iot-security-whitepaper.pdf.

СОБЫТИЯ РЫНКА

| СОТРУДНИК КОМПАНИИ АО «ПРОТОН-ЭЛЕКТРОТЕКС» СТАЛ ЛАУРЕАТОМ ВСЕРОССИЙСКОГО КОНКУРСА «ИНЖЕНЕР ГОДА – 2019» |

В номинации «Инженерное искусство молодых» и направлении «Радиотехника, электроника, связь» победил ведущий инженер-исследователь АО «Протон-Электротекс» Денис Олегович Малый.

Конкурс проводится Российским и Международным Союзом научных и инженерных общественных объединений и Академией инженерных наук имени А. М. Прохорова.

Появление полного цикла производства приборов IGBT в корпусах MIFA и MIAA стало следствием активной деятельности Д. О. Малого. До этого подавляющая часть IGBT поставлялась в Россию из-за рубежа.

После получения образования Денис Олегович начинает работать в АО «Протон-Электротекс». За рекордные два года при поддержке коллег и руководящего состава компании выстраивается полный производственный цикл модулей IGBT, не имеющих аналогов на территории Российской Федерации. На данный момент основная деятельность Д. О. Малого направлена на подготовку кадров, исследования тенденций в области силовых полупроводниковых приборов и разработку новейшего оборудования мирового уровня.

Отдел разработки трудится над очередной новинкой, аналогов которой не найти на территории России.

www.proton-electrotex.com