ВТОРОЕ ПОКОЛЕНИЕ AURIX: КОМПЛЕКСНАЯ БЕЗОПАСНОСТЬ ДЛЯ АВТОМОБИЛЯ БУДУЩЕГО

ДЭВИД ВЕРТВЕЙН (DAVID WERTHWEIN)
ПЕРЕВОД: ВЛАДИМИР РЕНТЮК

Ремень безопасности, антиблокировочная тормозная система, система курсовой устойчивости (активная система безопасности автомобиля) — долгое время это были ключевые слова, которые характеризовали технологии, сделавшие управление транспортными средствами более комфортным и безопасным. Однако используемые в настоящее время технологии, такие как сетевое взаимодействие подключенного транспортного средства и беспилотные автомобили, осуществляющие движение без водителя, привели к тому, что автомобиль стал неотъемлемой частью «Интернета вещей». В связи с этим возросли требования к безопасности такого транспортного средства, а соответствующие решения уже не только разработаны, но и доступны.

Английский язык, в отличие от немецкого и русского, проводит различие между двумя понятиями, которые мы определяем как безопасность, — safety и security. Мы должны согласиться, что для мира автомобилей такое разделение является достаточно точным. С точки зрения системы и водителя (safety) подразумевает «эксплуатационную безопасность». В данном контексте система считается безопасной, если гарантируется физическая целостность пользователя и других людей, например пассажиров. Следовательно, неисправность, представляющая опасность для человека и окружающей среды, должна быть исключена. Также это называется «функциональной безопасностью». В автомобильном секторе индустрии такое понятие определяется стандартом ISO 26262[1]. Что касается рисков, то системе присваивается определенный класс безопасности по ASIL (от англ. Automotive Safety Integrity Level)[2], и в соответствии со стандартом конкретный класс определяет качественные и количественные цели для каждого уровня безопасности.

Термин же security, напротив, в большей степени подразумевает уровень защиты от воздействия внешних угроз. В автомобильном секторе это прежде всего относится к системам и данным, то есть к вопросам, связанным уже с кибербезопасностью.

[1] В РФ действует стандарт ГОСТ Р ИСО 26262-1-2014 «Дорожные транспортные средства. Функциональная безопасность. Часть 1. Термины и определения», который идентичен международному стандарту ISO 26262-1:2011. — Прим. пер.

[2] ГОСТ Р ИСО 26262-1-2014 определяет класс безопасности по ASIL как уровни полноты безопасности автомобиля (УПБА). — Прим. пер.

В контексте этого понятия разработчику необходимо принять соответствующие меры, гарантирующие, что программный код, динамические данные автомобиля и сведения, представляющие интеллектуальную собственность и личную информацию, не смогут быть скопированы или обработаны незаконно. Необходимая правовая основа обеспечивается общеевропейским регламентом о защите персональных данных — European General Data Protection Regulation (GDPR), который вступит в силу 25 мая 2018 г.

Как известно, ключевую роль в электронных системах (рис. 1) играет микроконтроллер. Помимо контроля и управления автотранспортным средством, он отвечает за вопросы мониторинга. В идеале микроконтроллер, соответствующий требованиям комплексной безопасности (в контексте safety/security), в автопроме также может гарантировать определенный уровень комплексной безопасности и других компонентов в системе автомобиля.

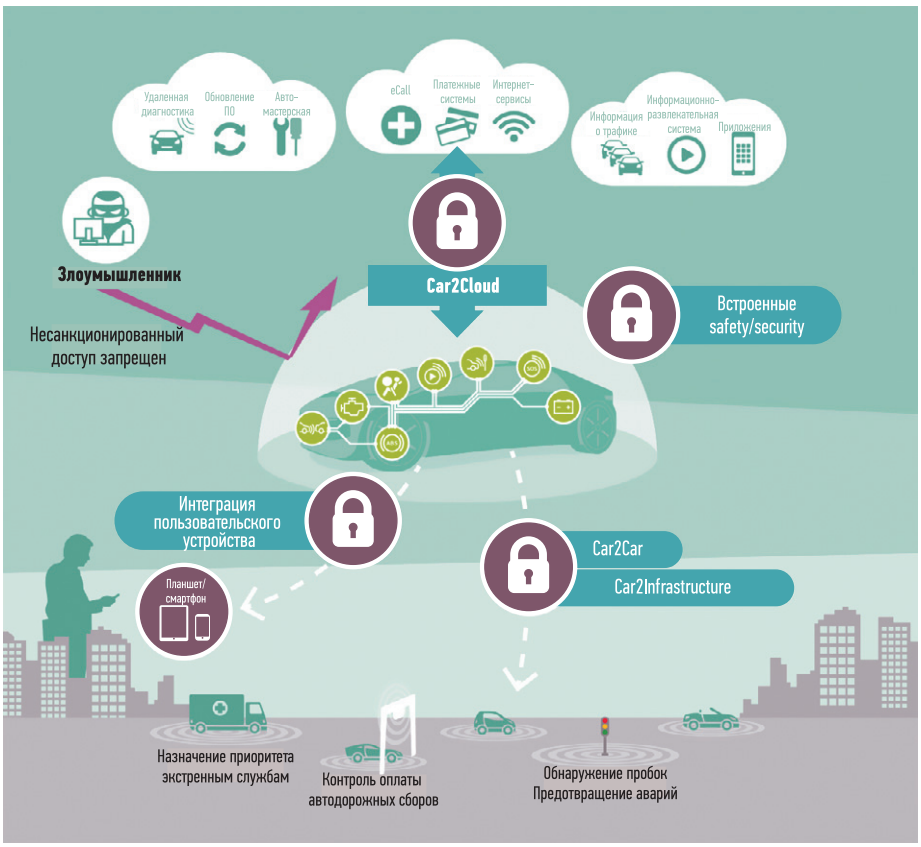

РИС. 1. ▲ Система безопасности автомобиля

ПРОБЛЕМЫ КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ АВТОМОБИЛЬНЫХ МИКРОКОНТРОЛЛЕРОВ

AURIX — это семейство микроконтроллеров компании Infineon, удовлетворяющее потребности автовладельцев с точки зрения обеспечения комплексной безопасности, реализуя ее в рамках как security, так и safety. Эти требования предусмотрены в стандарте ISO 26262 и реализуются с помощью ключевых компонентов микроконтроллера, т. е. центрального процессора, встроенной памяти и периферийных интерфейсов. Фактические уровни риска определяются оценкой риска, по результатам которой присваивается один из четырех классов ASIL. Микроконтроллеры AURIX поддерживают наивысший класс ASIL — уровень ASIL D[3].

Этот уровень защиты осуществлен с помощью встроенного модуля аппаратной защиты (hardware security module, HSM) и особой схемы включения независимых дублирующих вычислительных ядер (lockstep cores) контроллера AURIX, что предоставляет разработчику решение по типу «все-в-одном». Поскольку микроконтроллер и все предлагаемые им функции подключены к интегрированному на чипе HSM, он гарантирует комплексную безопасную вычислительную платформу в контексте safety/security. HSM имеет собственную флэш- и оперативную память для хранения приложений безопасности, а также ускоритель AES (Advanced Encryption Standard — симметричный алгоритм блочного шифрования, принятый в качестве стандарта шифрования правительством США) и собственный генератор истинно случайных чисел[4]. Поэтому может полностью шифровать данные и гарантировать безопасную связь и аутентификацию блока управления двигателем (иммобилайзер блокирует основные функции автомобиля при использовании несогласованного ключа). Благодаря HSM можно безопасно загружать микроконтроллер, что предохранит его от атак вирусов и троянов. HSM отделен от остальной архитектуры TriCore брандмауэром, т. е. обеспечен доверенной средой исполнения программ и команд.

ОСОБЕННОСТИ ВТОРОГО ПОКОЛЕНИЯ AURIX

В настоящее время ожидается выход в свет второго поколения контроллеров AURIX (TC3xx, рис. 2), которое будет постепенно заменять первое, уже сыгравшее свою важную роль. В контроллерах второго поколения предлагается до шести независимых встроенных ядер TriCore с полной тактовой частотой 300 МГц. Производительность процессора находится на уровне до 4000 DMIPS, что более чем в 2 раза выше, нежели у контроллеров предыдущего поколения (до 1600 DMIPS). Высокая масштабируемость в виде отдельных вариантов исполнения, которые, например, отличаются по флэш-памяти (до 16 Мбайт), встроенной оперативной памяти (до 6,9 Мбайт), типу корпуса и функций интерфейса, гарантирует, что для каждого приложения может быть выбран наиболее подходящий чип.

[3] По ГОСТ Р ИСО 26262-1-2014 уровень полноты безопасности автомобиля, для которого значение УПБА, равное D, является наиболее строгим уровнем, а значение УПБА, равное A, — наименее строгим. — Прим. пер.

[4] Генераторы истинно случайных чисел реализуются не на программной основе, а на физической, для этой цели могут использоваться природные надежные источники энтропии, например теплового шума или дробного шума полупроводниковых переходов. — Прим. пер.

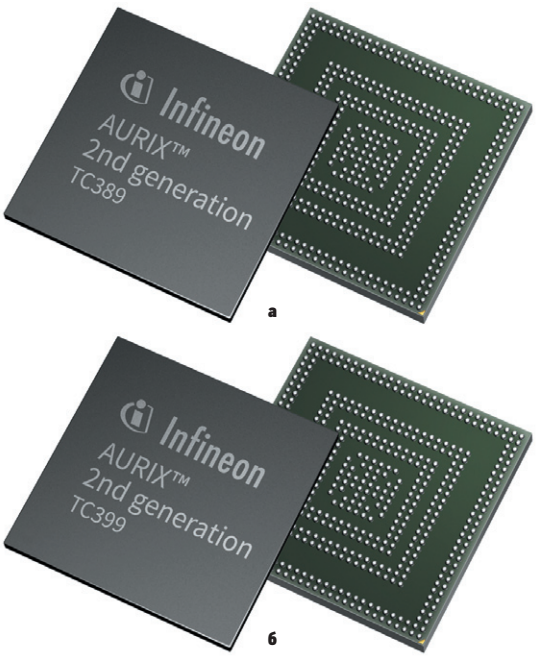

РИС. 2. ▲ Внешний вид микроконтроллеров AURIX: а) TC389; б) TC399

В самом продвинутом варианте микроконтроллера TC39x четыре из шести процессорных ядер имеют дополнительное дублирующее ядро (lockstep). Оно предлагает общую производительность процессора на уровне 2700 DMIPS — в 3 раза больше, чем у предыдущего поколения (до 900 DMIPS). Таким образом, последнее поколение AURIX устанавливает своеобразные реперные показатели с точки зрения производительности компьютерных вычислений в одном интегральном чипе, который, в частности, может использоваться для обеспечения функциональной безопасности по нормам стандарта ISO 26262. При этом вполне достижима разработка приложений, классифицированных как ASIL D — по самому высокому классу безопасности.

В отличие от первого поколения модуль аппаратной защиты HSM теперь реализован во всех вариантах исполнения TC3xx. Кроме того, его функции расширены и улучшены: новые асимметричные ускорители шифрования позволяют удовлетворить самые высокие требования EVITA (E-safety Vehicle Intrusion proTected Application)[5] и поддерживают не только безопасную связь на уровне автотранспортного средства, но и необходимую аутентификацию, что помогает предотвратить аппаратное манипулирование.

Поддержка SOTA при работе с eMMC и A/B-банками eFlash-памяти

Большие изменения коснулись и интерфейсов: новое поколение микроконтроллеров AURIX (TC3xx) имеет интерфейс eMMC для связи с внешней флэш-памятью. Благодаря наличию такого локального хранилища данных поддерживается и архитектура SOTA (software-over-the-air — передача программного обеспечения (ПО) по радиоканалу). Альтернативно можно использовать обмен A/B-банками eFlash-памяти. В этом случае обновления для ПО можно загрузить в блок управления автомобилем через беспроводное интернет-соединение. Владельцу автомобиля больше не требуется обращаться в автомастерскую, чтоб обновить прошивку ПО: он может выполнять эту задачу, даже не выходя из собственного гаража, через локальную сеть WLAN, и тем самым избежать возможных дорогостоящих действий из-за отзыва автомобиля по причине программного сбоя.

Использование радара

Еще одна новая особенность — наличие радиолокационного компонента. Его технологическая система с двумя специализированными блоками обработки сигналов (signal processing unit, SPU), работающими на частоте 300 МГц, позволяет использовать алгоритмы радаров следующего поколения, а значит, и все радиолокационные приложения — от системы контроля слепых зон автомобиля до новейших систем фронтальных и угловых радаров. Радиолокационные радиочастотные чипы легко подключаются к устройству через специализированные радиолокационные интерфейсы на основе протокола интерфейса LVDS IEEE1596-3. Таким образом, полностью автономная смена полосы движения и автоматическое поддержание дистанции могут быть интегрированы как основные функции в новые системы управления транспортным средством. Дополнительные интерфейсы связи второго поколения AURIX содержат интерфейс Gigabit Ethernet, каналы CAN-FD, соответствующие требованиям стандарта ISO 11898-1[6], и LIN-каналы.

Самая полная версия нового семейства — TC39x с встроенной флэш-памятью 16 Мбайт и, возможно, в корпусах BGA-292 или BGA-516 — уже доступна в качестве опытного образца, как и оценочные комплекты для проверки общих технических решений. Полная сертификация семейства данных продуктов запланирована компанией Infineon на первый квартал 2019 г.

ВОПРОСЫ КООПЕРАЦИИ ПРИ РАЗРАБОТКЕ ПРОЕКТОВ

Эксперты ожидают, что продукты и технологии, предназначенные для полностью автоматизированного управления беспилотными транспортными средствами, будут готовы к полномасштабному производству к середине следующего десятилетия. Благодаря сочетанию обеих составляющих безопасности, safety и security, а также многоядерной архитектуры второе поколение микроконтроллеров AURIX (TC3xx) закладывает основы для целого ряда промышленных и автомобильных приложений. Но компаниям, стремящимся занять ведущие позиции в этой области, нужны не только безопасные со всех точек зрения продукты.

Для того чтобы гарантировать полную безопасность данных и функциональную безопасность во всем конечном приложении, предприятия должны решать сложные проблемы, обычно выходящие за рамки их традиционных знаний. Например, уровень разработки ПО слишком высок, чтобы с ним могли справиться обычные специалисты. Однако новые методы сотрудничества позволяют объединить ноу-хау и значительно облегчить процесс проектирования. Идея экосистемы, которая получает распространение в секторе ПО на протяжении многих лет, сегодня становится характерной чертой и развития электроники. В частности, компания Rutronik тесно сотрудничает с сетью поставщиков услуг по проектированию, а также систем и компаний, выпускающих ту или иную оснастку. Партнером по выбору помощников в этом секторе, а также по вопросам функциональной безопасности и защиты данных для решений на базе встраиваемой электроники является системный поставщик HITEX, эксперт по проектам AURIX. ⬣

[5] Цели проекта EVITA заключаются в разработке модельной сети тестирования сенсорных сетей обеспечения безопасности автомобилей. — Прим. пер.

[6] В РФ действует ГОСТ Р ИСО 11898-1-2015 «Транспорт дорожный. Местная контроллерная сеть (CAN). Часть 1. Канальный уровень и передача сигналов», идентичный международному стандарту ИСО 11898-1:2003 с поправкой от 2006 года. — Прим. пер.