Внедрение инноваций в приложения IoT: исследование пяти главных проблем с помощью пяти основных принципов IoT

Сук Хуа Вонг (sook-hua_wong@keysight.com)

В статье рассказывается о важности Интернета вещей (Internet of things, IoT), связанных с этой технологией пяти основных принципах решения технических проблем и общих требованиях при проектировании IoT-устройств.

Интернет вещей (IoT) быстро развивается. По данным IoT Analytics [1], количество подключённых устройств в 2019 году превысило первоначальные прогнозы на 14% и достигло 9,5 млрд. Три основных причины: взрывной рост количества бытовых приборов, гораздо большее, чем ожидалось, число сотовых IoT/M2M-соединений и значительное увеличение объёма подключённых устройств в Китае благодаря правительственным инициативам.

Экспоненциальный рост продолжится в течение следующих нескольких лет. К 2025 году количество подключённых устройств достигнет 28 млрд. Соответствующие технологии уже интегрированы в электронику и предметы одежды. На каждого жителя Земли будет приходиться 26 «умных» предметов [2]. 75% автомобилей будут иметь оборудование для соединения с Интернетом [3]. Прогнозируется, что к 2025 году доходы, связанные с применением IoT в здравоохранении, превысят $135 млрд [4].

IoT разносторонне развивается: от потребительских приложений, таких как устройства для умного дома и носимая электроника, до критически важных приложений, обеспечивающих общественную безопасность, промышленную автоматизацию, реагирование на чрезвычайные ситуации, а также работу беспилотных транспортных средств и Интернета медицинских вещей (IoMT). Для таких приложений важны удобство применения, низкая стоимость, длительное время работы устройств от батареи и широкодоступная инфраструктура общего пользования, позволяющая улучшить функциональную совместимость, взаимную связь между устройствами, мониторинг и управление различными ответственными устройствами и системами в режиме реального времени.

По мере распространения критически важных приложений устройства и системы IoT должны становиться всё более надёжными, чтобы выдерживать жёсткие условия эксплуатации.

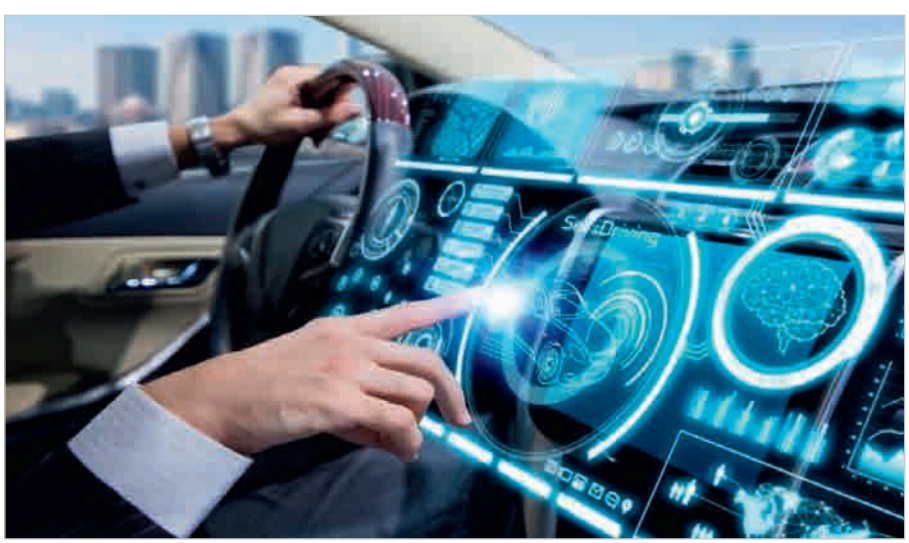

Рис. 1. Автомобиль оснащён интерактивной приборной панелью, которая имеет доступ в Интернет и общается с другими подключёнными устройствами

Большому потенциалу сопутствуют большие проблемы

IoT приносит выгоду потребителям и создаёт новые бизнес-возможности для предпринимателей. Однако для этого требуются надёжное оборудование и стабильная инфраструктура.

Система экстренного реагирования. Что случится, если беспроводной датчик, контролирующий давление в магистральном газопроводе, выйдет из строя из-за перебоя в электроснабжении? Газопровод может взорваться, если своевременно не отреагировать на увеличение давления.

Цифровое здравоохранение. Устройства удалённого мониторинга пациентов позволяют осуществлять наблюдение вне больницы, что расширяет возможности медицинского обслуживания и снижает стоимость оказания медицинской помощи. Однако сами устройства должны работать в любых условиях, например на переполненном стадионе или труднодоступном для передачи сигналов подземном складе. Приём сигнала через бетонные конструкции и помехи от окружающих устройств не должны влиять на нормальную работу устройства мониторинга.

Умный счётчик. На каждом удалённом объекте могут быть установлены сотни тысяч крошечных интеллектуальных счётчиков, которые должны бесперебойно собирать и передавать данные о потреблении ресурсов коммунальным службам. Любой сбой в работе такого счётчика приведёт к ошибкам в контроле потребления, вызовет потерю доходов и потенциально ухудшит репутацию коммунальной компании.

Подключённый автомобиль. Подключённый автомобиль, показанный на рисунке 1, – чрезвычайно удобная вещь. Но он также подвергает нас различным рискам. Если при создании системы беспроводной связи не была обеспечена достаточная безопасность, то хакер сможет одним нажатием кнопки найти и незаметно угнать машину.

Инженеры и конструкторы, работающие над этими критически важными системами или устройствами, сталкиваются с серьёзными техническими проблемами. Они должны принимать важные решения по проектированию и испытаниям, а также идти на компромиссы, начиная с ранней стадии разработки и заканчивая окончанием производства.

Решение технических проблем с помощью пяти основных принципов IoT

Решение многосторонних технических проблем в устройствах и системах IoT на протяжении всего жизненного цикла продукта требует комплексного подхода. Проблемы, которые необходимо учитывать при проектировании, можно обобщить с помощью пяти принципов IoT (см. табл.).

1. Коммуникация

Коммуникация – это возможность обеспечить бесперебойный двунаправленный поток информации для устройств, инфраструктуры, облака и приложений. Достижение качественной системы обмена сообщениями является одной из главных проблем, с которой сталкиваются инженеры, потому что система беспроводной связи очень сложна, а высокая загрузка спектра ещё больше усложняет работу. Ожидается, что критически важные устройства IoT будут надёжно работать без сбоев даже в самых сложных условиях. Быстрое развитие стандартов беспроводной связи усугубляет ситуацию, и поэтому инженеры вынуждены постоянно решать возникающие проблемы, чтобы идти в ногу с новейшими технологиями и обеспечивать бесперебойную работу устройств по всей экосистеме IoT.

Решение проблем взаимной коммуникации требует тщательного выбора конструкторских и испытательных решений, которые должны быть очень гибкими, легко конфигурируемыми и модернизируемыми для удовлетворения будущих потребностей. Решение должно быть достаточно гибким, чтобы тестировать устройства с поддержкой большого числа радиоформатов, иметь доступ к характеристикам устройства в реальных рабочих режимах, а также поддерживать тестирование по радиоэфиру в режиме сигнализации без необходимости использования специального драйвера чипсета тестируемого устройства. Предпочтительно, чтобы система была также простой, недорогой и могла использоваться как в исследованиях и разработках, так и на производстве для повышения эффективности и сведения к минимуму проблем корреляции измерений на различных этапах проектирования. Спрос на устройства IoT будет расти в геометрической прогрессии. Производителям необходимо иметь хорошо масштабируемую, экономичную и надёжную производственную испытательную систему, которая легко справляется с растущими объёмами выпуска, обеспечивая при этом высокое качество продукции.

2. Бесперебойность

Бесперебойность связана с надёжностью работы и увеличением срока службы батареи устройства. Время работы от батареи – один из наиболее важных факторов для устройств IoT. Длительный срок службы батареи является гигантским преимуществом бытовых устройств IoT. От промышленных устройств обычно ожидают срока службы в 5 или 10 лет. Для медицинских устройств, таких как кардиостимулятор, срок службы может стать вопросом жизни и смерти пациента. Об отказе батареи не может быть речи.

Для удовлетворения требования к длительному сроку службы батареи конструкторам интегральных схем (ИС) необходимо разработать ИС с режимом глубокого сна, в котором потребляется очень малый ток, понижается тактовая частота и сокращается набор команд. Также следует реализовать возможность работы при низком напряжении батареи. Группы стандартов беспроводной связи, такие как NB-IoT, LTE-M, LoRa и Sigfox, определяют новые режимы работы с низким энергопотреблением. Эти режимы предлагают ограниченное время активной работы при сохранении низкого энергопотребления. Разработчики, интегрирующие в конечный продукт компоненты измерения, обработки, управления и связи, должны знать, как ведут себя периферийные устройства, как они потребляют энергию. Обладая этими знаниями, можно оптимизировать микропрограммное и программное обеспечение продукта, упростить эксплуатацию и снизить потребляемый ток. Все эти действия требуют эффективных измерительных инструментов, которые предоставят данные для глубокого анализа энергопотребления устройства.

Пять основных принципов решения технических проблем IoT

Коммуникация	IoT-устройства должны подключаться к другим IoT-устройствам, облачным средам и оборудованию по всему миру.
Бесперебойность	Для успешной работы устройства должны иметь батареи с длительным сроком службы.
Соответствие	IoT-устройства должны соответствовать международным нормативным документам.
Совместимость	IoT-устройства должны стабильно взаимодействовать в переполненной среде IoT.
Кибербезопасность	Данные должны быть защищены от киберугроз.

3. Соответствие

Понятие «соответствия» заключается в том, чтобы устройства IoT отвечали требованиям стандартов радиосвязи и другим международным нормативным документам перед тем, как будут представлены на рынке. Есть две основные категории испытаний на соответствие: испытания на соответствие стандартам радиосвязи и совместимости несущих, а также испытания на соответствие нормативным требованиям. В последнюю категорию входят измерения радиочастотных характеристик, проверка электромагнитной совместимости и измерение удельного коэффициента поглощения электромагнитной энергии (SAR). Инженеры-проектировщики часто пытаются соблюсти жёсткие сроки вывода продукции на рынок и обеспечить беспрепятственный выход на мировой рынок, соблюдая при этом новейшие нормативные требования. Частые обновления нормативных документов усложняют ситуацию ещё больше. Примеры требований соответствия нормативным документам приведены на рисунке 2.

Снизить риск непрохождения тестирования на соответствие и не срывать график выпуска продукции проектировщики могут с помощью вложения средств в собственные решения по тестированию. Таким образом можно будет проверять устройство на каждом этапе проектирования и исправлять проблемы на ранних стадиях. При выборе системы предварительного тестирования необходимо учитывать, какое оборудование будет использоваться в испытательной лаборатории в процессе финальных испытаний на соответствие. Это поможет обеспечить корреляцию измерений и снизить риск непрохождения тестов. Испытания на

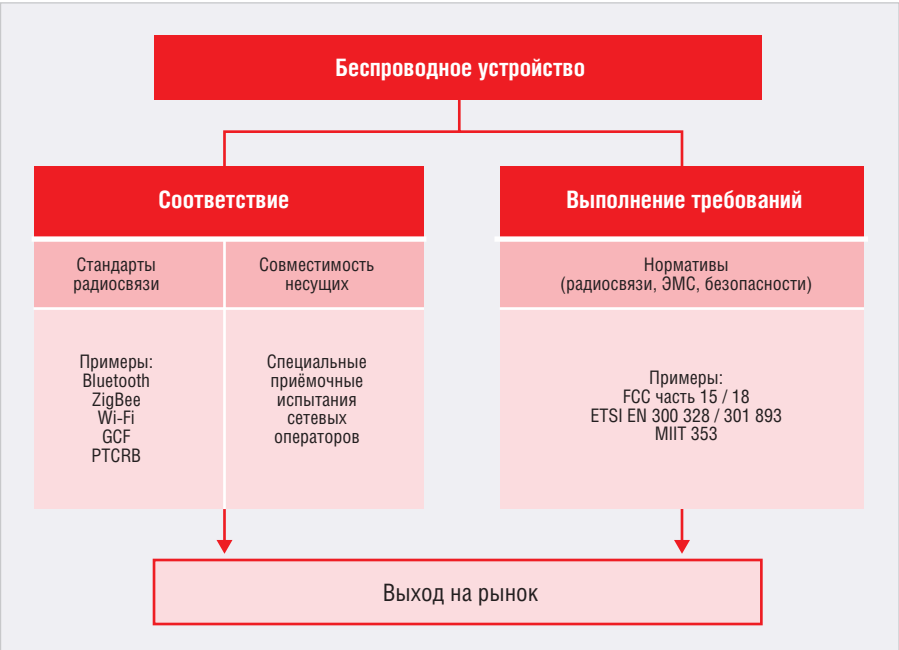

Рис. 2. Требования к устройствам IoT, соблюдение которых необходимо проверять

соответствие стандартам – очень сложная задача, занимающая много времени. На её выполнение вручную уходят дни и недели. Выбор автоматизированной системы тестирования поможет сэкономить время и ускорить вывод продукции на рынок.

4. Совместимость

Совместимость – способность беспроводного устройства надёжно работать при наличии помех от других устройств. С выходом на рынок миллиардов устройств перегруженность радиоканалов становится проблемой, которая с каждым днём будет только усугубляться. Чтобы решить проблемы перегрузки в беспроводных сетях, органы стандартизации разработали методики тестирования и оценки работы устройства в присутствии других сигналов. Например, в Bluetooth® адаптивная скачкообразная перестройка частоты (AFH) позволяет устройству Bluetooth исключать каналы, в которых происходит большое количество конфликтов данных (см. рис. 3). Существуют и другие методы предотвращения конфликтов, такие как механизм «Слушай, прежде чем сказать» (Listen Before Talk, LBT) и совместное предотвращение коллизий (CCA) для повышения эффективности передачи данных. Эффективность передачи в среде смешанных сигналов неизвестна. Когда сигналы различных радиоформатов не могут обнаружить друг друга, происходят конфликты и потери данных.

Для потребительских приложений задержки и паузы в работе беспроводных гарнитур или носимой электроники раздражают, но всё же возникновение таких проблем допустимо. Потеря управляющего сигнала промышленным датчиком или прекращение работы инфузионного насоса из-за воздействия помех может привести к тяжёлым последствиям. Поэтому для измерения и оценки того, как устройство будет работать в условиях перегруженного спектра и наличия смешанных сигналов, крайне важно провести испытания на совместимость. IEEE предоставляет некоторые рекомендации в ANSI C63.27 (Американский национальный стандарт оценки совместимости беспроводных сетей) в отношении ключевых аспектов тестирования совместимости. Рекомендации включают в себя описание процессов оценки, измерительных схем и уровней тестирования на основе оценки риска. Производителям устройств настоятельно рекомендуется оценить потенциальные риски для функционирования беспроводного устройства при наличии нежелательных сигналов, обнаруженных в той же рабочей среде.

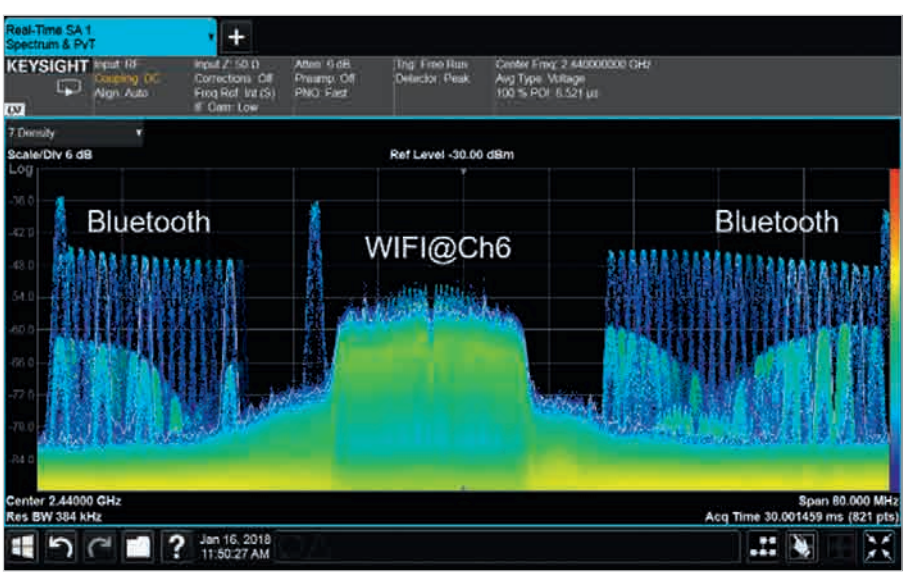

Рис. 3. Устройство Bluetooth обходит Wi-Fi-канал 6, чтобы избежать помех от сигнала Wi-Fi

5. Кибербезопасность

Расширение применения IoT в критически важных приложениях повышает значение кибербезопасности. В то время как кибератаки могут происходить на многих уровнях – от уровня устройства до уровня сети связи, облака или приложений, большинство традиционных средств защиты сосредоточены на обеспечении безопасности сети и облака. Про уязвимость оконечных точек и беспроводных сетей часто забывают. Технологии Bluetooth и WLAN считаются «зрелыми» и используются во множестве областей. Тем не менее для решения проблем, связанных с уязвимостями в беспроводной сети, мало что было сделано. Сложность этих беспроводных протоколов обуславливает в реализации радиоинтерфейсов устройств потенциальные уязвимости, которые позволяют хакерам получить доступ к устройству или взять его под контроль.

По данным IDC, 70% брешей в системе безопасности связаны с оконечными точками [5]. Для защиты IoT-устройств должны быть приняты дополнительные меры. Следует выявить уязвимости в беспроводной сети и обнаружить потенциальные точки проникновения в IoT-устройства. Устройства должны быть протестированы с использованием базы данных известных угроз и атак через беспроводной интерфейс. Так можно проверить реакцию устрой-

ства и выявить различные аномалии. База данных должна регулярно обновляться для защиты устройств от новых угроз.

Построение надёжного фундамента IoT на основе пяти принципов Интернета вещей

IoT открывает двери для новых применений и возможностей во многих отраслях промышленности. Также Интернет вещей ставит беспрецедентные задачи, которые требуют нового мышления, обеспечивающего соответствие требованиям по решению критически важных задач. Для успешного внедрения IoT от конструкторов и инженеров требуется преодолеть технические проблемы соблюдения пяти основных принципов, о которых было рассказано. Глубокое понимание технических проблем и знание ключевых аспектов проектирования и тестирования заложат прочный фундамент для внедрения и развёртывания экосистемы IoT. Правильные средства проектирования, проверки и испытаний на соответствие стандартам и требованиям производства на протяжении всего жизненного цикла продукта помогут гарантировать реализацию всех возможностей IoT.

Литература

1. IoT 2019 in Review. The 10 Most Relevant IoT Developments of the Year. URL: https://iot-analytics.com/iot-2019-in-review/.
2. A Guide to the Internet of Things. URL: https://www.intel.com/content/dam/www/public/us/en/images/iot/guide-to-iot-infographic.png.
3. The «connected car» is creating a massive new business opportunity for auto, tech, and telecom companies. URL: https://www.businessinsider.com/connected-car-forecasts-top-manufacturers-2015-2.
4. 7 Staggering Stats on Healthcare IoT Innovation. URL: https://medium.com/datadriveninvestor/7-staggering-stats-on-healthcare-iot-innovation-fe6b92774a5c.
5. IDC Says 70% of Successful Breaches Originate on the Endpoint. URL: https://journalofcyberpolicy.com/2019/09/09/idc-says-70-successful-breaches-originate-endpoint/.

НОВОСТИ МИРА

MIPS-архитектура RISC-процессоров «пошла по рукам»

По информации агентства Reuters, попытка американских властей предотвратить попадание технологии RISC-процессоров с архитектурой MIPS в «чужие руки» не увенчалась успехом.

В 2017 году компания IMAGINATION, владевшая данной технологией, была разделена, и часть, обладавшая лицензионными правами, была куплена калифорнийским инвестфондом Tallwood Ventures, принадлежавшим Диосдадо Банатао (Diosdado Banatao), который в 80-е годы был сооснователем таких компаний, как CHIPS & TECHNOLOGIES и S3 GRAPHICS. После серии перепродаж правом лицензирования MIPS-архитектуры владеет компания, зарегистрированная на Самоа – Prestige Century Investments, передавшая это право своей шанхайской «дочке» CIP United.

Новостная рассылка проекта «Мониторинг рынка электроники»