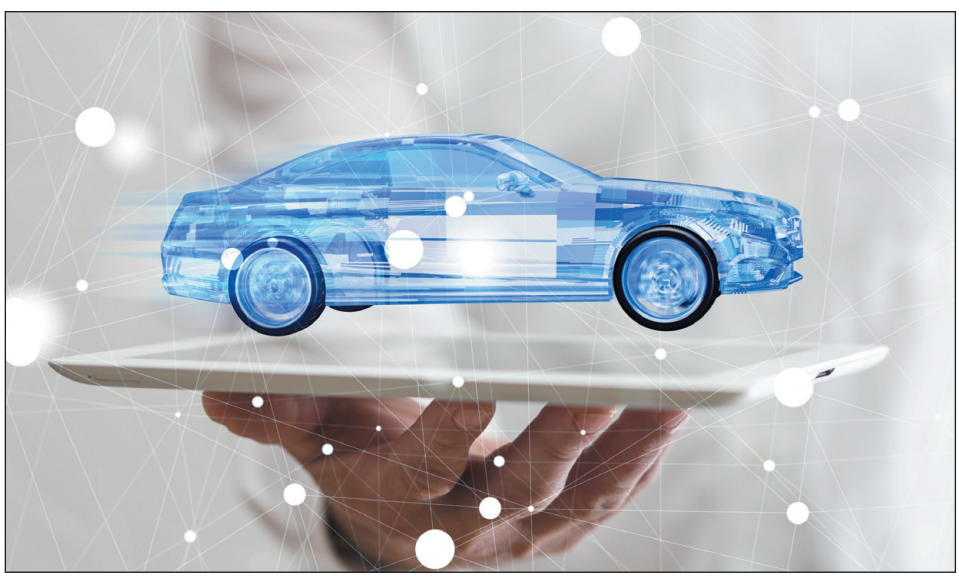
Обновления прошивки и ПО автомобилей по беспроводным каналам связи:

«умные» обновления для «умных» автомобилей

В автомобильной индустрии регулярные обновления прошивки и программного обеспечения в первую очередь направлены на повышение уровня функциональности, безопасности и надежности автомобилей. Однако тут есть проблема — для установки обновлений транспортные средства, как правило, требуется доставить в автомастерскую, авторизированную для данной процедуры. Обновления по радиоканалу беспроводной сети должны покончить с этой рутиной. Владельцы автотранспортных средств наконец-то смогут так же просто, как и на своих смартфонах, загружать последние сборки специального и версии типового программного обеспечения, причем в любое время и в любом месте.

Бернд Вондратчек (Bernd Wondratschek)
Перевод: Владимир Рентюк

Передача обновлений по технологии беспроводной связи OTA (OTA — Over-the-air) означает, что обновления прошивки и программного обеспечения больше не выполняются по кабелю, а передаются по беспроводной сети. Это может быть достигнуто с использованием различных стандартов, включая сотовую радиосвязь и WLAN, а также по Bluetooth и NFC[1], например непосредственно на зарядных станциях или автозаправках. В автомобиле обновления в первую очередь затрагивают блоки управления двигателем ECU (ECU — engine control unit) и информационно-развлекательную систему. В то время как обновления для блоков управления двигателем обычно закрывают бреши в системе безопасности и повышают его производительность, обновленная информационно-развлекательная система способствует повышению комфорта и удобства индивидуального использования.



[1] NFC — Near field communication («связь ближнего поля»), технология беспроводной передачи данных малого радиуса действия, которая дает возможность обмена данными между устройствами, находящимися на расстоянии до 4 см.

По мере того как все больше новых автомобилей поступает на рынок со встроенными электронными системами управления двигателями, причем с интенсивным использованием программного обеспечения, возрастают и требования к обслуживанию программного обеспечения. Так, согласно исследованию, проведенному Национальной администрацией безопасности дорожного движения США (US National Highway Traffic Safety Administration, NHTSA), в 2015 году 15% от общего числа отзывов о безопасности транспортных средств в стране связаны с ошибками программного обеспечения. Устранение таких ошибок гораздо сложнее для транспортных средств, чем, например, для смартфонов. Если в транспортном средстве обнаружена ошибка или критическая уязвимость, связанная с программным обеспечением, ее необходимо устранять в специализированной мастерской. Это единственное место, где эксперты могут предоставлять обновления от поставщиков программного обеспечения, обычно OEM-производителей, и поступает оно к ним через кабельное соединение. Однако это не только стоит времени и нервов автовладельцам, но и довольно дорогое удовольствие для производителей оригинального оборудования.

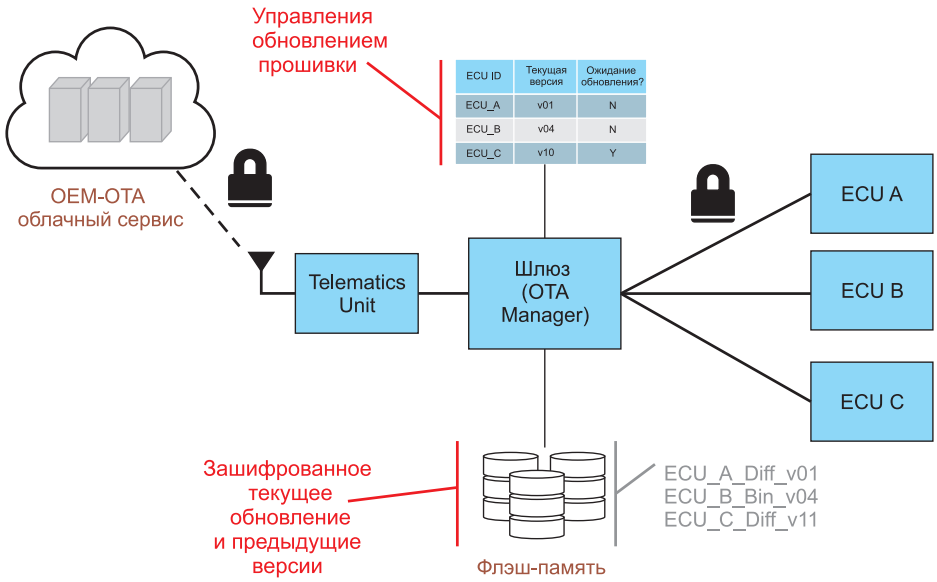


Рис. 1. Презентация функционирования технологии OTA в автомобиле (предоставлено компанией Rutronik)

Главное условие для технологии OTA — это сетевые транспортные средства

Главная возможность, позволяющая получать обновления по радиоканалу для современных более интеллектуальных автомобилей, — наличие в них сотового радиооборудования. Здесь важном моментом является постановление ЕС, известное как eCall, которое как раз и требует установления систем сотовой радиосвязи в автомобилях. Документ гласит, что с марта 2018 года все новые модели транспортных средств в Европейском союзе должны быть оснащены «функцией экстренного вызова» (это, собственно, и есть система eCall). Эта специальная функция в случае аварии автоматически вызывает службы экстренной помощи, используя европейский номер службы экстренной помощи 112. Но она также предоставляет изготовителям и продавцам автотранспортных средств базовый вариант для связи и получения обновлений через технологию OTA. Следовательно, тут можно сэкономить, поскольку интерфейс OTA позволяет через магазин приложений (apps) создавать и активировать новые функции и приложения, если это, конечно, предусматривает само оборудование.

Преимущества технологии OTA для получения обновлений очень существенны. Пользователям теперь не нужно посещать автомастерскую для получения обновлений, и вместе с тем они имеют все преимущества от установки новейшего специализированного и встроенного программного обеспечения и связанных с ним улучшений, например в виде постоянно обновляемых дорожных карт и новых приложений. В свою очередь изготовителям и поставщикам доступно больше информации о пользователях транспортных средств и конфигурации конкретного автомобиля, они могут избежать затрат на отзыв автомобилей из-за тех или иных багов в программном обеспечении и обеспечить безопасность транспортных средств на более высоком уровне.

Передача и распространение обновлений

Целью технологии OTA (рис. 1), как уже было сказано, является замена передачи обновлений по кабелю, которую необходимо выполнить в автомастерской, на мобильное соединение между сервером OEM и телематическим блоком автомобиля. Однако напрямую система eCall не подходит для этого, поскольку не может передавать какие-либо иные данные, за исключением экстренных вызовов. А потому для транспортного средства потребуется отдельная SIM-карта, или оно должно получить доступ к соединению через точку доступа смартфона или сеть WLAN. Если соединение установлено, то здесь уже OTA Manager, действуя в данном случае как шлюз, может инициировать процесс приема обновления.

Основа всего — безопасность и защита

В дополнение ко многим неоспоримым преимуществам обновления по технологии OTA несут в себе и значительный риск. Поскольку в ней используются каналы связи, к которым можно подключаться, крайне важно защитить передачу пакетов данных, так как в противном случае сторонние, неуполномоченные лица, а попросту злоумышленники, могут получить доступ к важным функциям или данным автомобиля.

Поэтому меры защиты и обеспечения безопасности становятся важными аспектами успеха внедрения технологии OTA. Необходимо принять те или иные меры, гарантирующие безопасность маршрута передачи безопасной реализации процесса обновления. Сказанное выше предусматривает защиту маршрута передачи с использованием различных механизмов, таких как TLS[2], HTTPS (HyperText Transfer Protocol Secure — безопасный протокол передачи гипертекста), идентификация пользователя, VPN[3] и E2EE[4]. Если этот процесс недостаточно защищен, могут иметь место так называемые атаки посредника, или атаки «человека посередине»[5]. В рассматриваемом случае непринятие должных мер приводит к компрометации канала связи, при которой хакер, подключившись к каналу между источником обновлений (компанией — разработчиком ПО) и приемником (автомобилем), осуществляет вмешательство в протокол передачи, удаляя или искажая информацию. Здесь может иметь место внесение нарушений в работу электрической системы, кража интеллектуальной собственности, слежка за водителем, остановка двигателя или любое манипулирование функциями транспортного средства.

Процессы хранения и выполнения обновления, как правило, также актуальны с точки зрения безопасности. Чтобы предотвратить манипуляции с программным обеспечением и обеспечить подлинность и целостность данных, пакет программного обеспечения должен быть подписан криптографически. В структуре аппаратного обеспечения эту функцию безопасности может взять на себя

[2] TLS — transport layer security, протокол защиты транспортного уровня, как и его предшественник SSL (secure sockets layer — слой защищенных сокетов), представляет собой криптографические протоколы, обеспечивающие защищенную передачу данных между узлами в сети Интернет.
[3] VPN — Virtual Private Network, виртуальная частная сеть — обобщенное название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети, например Интернет.
[4] E2EE — end-to-end encryption, сквозное шифрование, также известное как оконечное шифрование, — способ передачи данных, в котором только пользователи, участвующие в общении, имеют доступ к сообщениям.
[5] Под термином «человек посередине» (в английской терминологии «Man in the middle», MITM) подразумевается вид атаки в криптографии, когда злоумышленник тайно ретранслирует и при необходимости изменяет связь между двумя сторонами, которые считают, что они непосредственно общаются друг с другом.

Таблица. Описание различий систем (F)OTA в смартфоне и автомобиле

Наименование устройства	Смартфон	Автомобиль
(F)OTA	Обновление операционной системы (IOS, Android и т. д.). Назначение — устранения проблем с безопасности и повышение производительности. Установка мобильных приложений для повышения возможностей индивидуального использования смартфона	Обновление блоков управления двигателем (ECU). Назначение — закрыть бреши в безопасности и улучшить производительность двигателя. Установка приложений и обновление информационно-развлекательной системы для повышения возможностей и улучшения их индивидуального использования

специальный аппаратный модуль безопасности HSM (HSM — hardware security module).

Надоедает ждать установки обновлений? Есть варианты

В рамках рассматриваемой проблемы существует еще несколько важных моментов, которые следует иметь в виду и не забывать о них. Речь идет о времени получения и продолжительности обновлений. Дело в том, что блоки управления двигателем (ECU) автомобиля могут получать обновления только в безопасном для водителя и автомобиля состоянии, то есть при выключенном двигателе. Однако владельцы далеко не всегда намерены ждать окончания процесса обновления, они хотят использовать свое транспортное средство вне зависимости от длительности процедуры — сейчас и сразу. Таким образом, во избежание длительного простоя автомобиля процесс обновления должен проходить максимально удобно и незаметно для владельца транспортного средства.

Возможные решения включают применение систем с избыточной памятью, в которой будет храниться как новая прошивка, так и резервные копии старой. При таком подходе, если процесс обновления по той или иной причине успешно не завершен (спешащий по делам водитель сел за руль и завел машину), то функциональность транспортного средства сохраняется. Дальнейшая мера — это запланированные процессы обновления, которые происходят в желаемое время, обычно ночью, когда потребность в транспортном средстве, как правило, отсутствует.

Для того чтобы гарантировать более быструю загрузку, размер пакетов данных должен быть как можно меньше. Объем программного обеспечения значительно варьируется в зависимости от электроники управления двигателем и информационно-развлекательных систем, и если необходимо заменить весь код прошивки или программного обеспечения, то может быть создано несколько гигабайт данных. Однако это можно исправить путем сжатия пакетов данных с помощью дельта-кодирования, и вместо всего программного кода он будет содержать только изменения в предыдущей версии. Такой подход сокращает объем данных до нескольких сотен мегабайт.

Возможные решения от компании Rutronik

Уже сегодня компания Rutronik предлагает ряд решений для реализации OTA-обновления автомобиля, включая сотовые радиомодули (BT, NFC, 3G, 4G, Wi-Fi). Кроме того, доступны микроконтроллеры безопасности со встроенными модулями HSM, в том числе семейство AURIX компании Infineon и семейство SPC58 от компании STMicroelectronics, а также микросхемы безопасности и микросхемы для доступа к сети сотовой связи от обоих упомянутых поставщиков.

Помимо того, Rutronik предлагает своим клиентам и соответствующее ПО, например программное обеспечение облачного управления IoT Portal компании Telit. Оно специально предназначено для одновременного распространения программного обеспечения среди большого количества клиентов. Платформа может быть брендирована для различных целей и поставщиков, а также позволяет отправлять индивидуальные сообщения клиентам. При использовании функции Geofence («Геозона») передача программного обеспечения может быть ограничена определенной областью. Предусмотрены и обычные ограничения и типичные этапы развертывания ПО.

Учитывая изложенное, можно с уверенностью сказать, что клиенты, которые используют для разработки и продвижения своих продуктов постоянно растущий портфель предложений компании Rutronik, уже сейчас готовы к будущему автомобильной отрасли с обновлениями прошивки и программного обеспечения по технологии OTA. ■