



Las actualizaciones de tecnología OTA necesitan una arquitectura flexible

Un vehículo permanece estacionado durante la noche en un garaje, inmóvil hasta que su conductor regresa y lo lleva a su próximo viaje. Pero en lugar de solo esperar, este vehículo está ampliando sus capacidades, volviéndose más seguro, aumentando su inteligencia y aprendiendo a realizar funciones tan bien como los vehículos más nuevos que salen de las líneas de ensamblaje ese mismo día.

Esto es posible gracias a las actualizaciones de software con tecnología inalámbrica (OTA). Cuando se integra con la arquitectura del vehículo, la tecnología OTA permite que los fabricantes puedan evolucionar la seguridad activa, el infoentretenimiento y otros dominios de sus vehículos, en un forma elegante, escalable, de bajo riesgo y rentable, mucho después de que salen de fábrica.

Una arquitectura diseñada con cálculo centralizado y optimizada para tecnología OTA puede ayudar a garantizar que las actualizaciones de software y firmware se efectúen sin problemas y de forma segura, con la frecuencia que necesite la aplicación, la estrategia de los fabricantes de equipos originales y las preferencias de los consumidores. La tecnología OTA no solo es esencial para construir vehículos operados con software, sino que también abre el potencial para nuevos servicios innovadores, nuevas formas de ofrecer características y nuevos modelos de negocios, y brinda flexibilidad y elasticidad como nunca antes fue posible.

HACEMOS POSIBLE EL VEHÍCULO OPERADO CON SOFTWARE

Los grandes fabricantes de equipos originales están lanzando vehículos [operados mediante software](#), con la intención de ofrecer más características en una fecha posterior, al utilizar redes celulares o de wifi para hacer las entregas de actualizaciones [OTA](#) de software y firmware. Las funciones residen cada vez más en los sistemas complejos y críticos de seguridad, por lo que es imperativo que estas actualizaciones se efectúen con seguridad y confiabilidad.

Si bien la tecnología OTA se está volviendo cada vez más omnipresente, no es una capacidad que se pueda agregar sin más, sino que la arquitectura del automóvil debe diseñarse teniendo en cuenta esta tecnología. Para optimizar la tecnología OTA es clave centralizar el control de cálculos dentro del vehículo, de modo que las actualizaciones solo tengan que descargarse en esa ubicación central, en lugar de distribuirse a los sistemas en todo el vehículo.

Afortunadamente, las arquitecturas electrónicas del vehículo ya se están desplazando hacia la centralización. Por ejemplo, [Satellite Architecture de Aptiv](#) toma la inteligencia de los radares, las cámaras y otros sensores y la centraliza en un poderoso controlador de dominio. Este enfoque mantiene los sensores pequeños y livianos, lo cual mejora el empaquetado y la flexibilidad de diseño, y, a su vez, también permite que los fabricantes administren mejor la disipación del calor. Al mismo tiempo, Satellite Architecture habilita capacidades avanzadas en el control de dominio, tales como utilizar la fusión de sensores para unir las entradas de varios sensores en un modelo ambiental cohesivo.

Algún contenido de software o firmware se mantiene con el radar o la cámara, pero ese código rara vez necesita cambios en el campo. Las características y componentes del software se introducen en el cómputo central. Por ejemplo, el software de seguimiento que identifica a los objetos alrededor del vehículo y sigue sus movimientos.

Este enfoque mantiene bajos los costos, porque necesita menos recursos de ingeniería para verificar cualquiera de los cambios en el software.

Antes de que se actualice cualquier software, o que se “ilumine”, cada componente que se actualiza, debe pasar por un riguroso conjunto de condiciones de prueba para garantizar que funciona de manera apropiada. Por ejemplo, si el rastreador reside en sensores inteligentes, entonces cada sensor deberá volver a verificarse antes de que se implemente la actualización. De todas maneras, si el rastreador (u otros componentes del software afectados por una actualización) residen en el control de dominio, solo debe volver a verificarse el control de dominio. Esto simplifica el proceso e insume menos recursos y tiempo.

Cada actualización OTA tendrá algunos costos asociados a ellas que van más allá de la nueva verificación, incluidos los costos de cargar el software en la nube, de la administración de la nube, del cifrado, de la descarga y del uso del tiempo en línea. Simplificar aquellas actualizaciones tanto como sea posible puede ayudar a mantener bajo los costos.

Si las actualizaciones no se pueden centralizar por completo, aún tiene sentido designar un maestro que controle las actualizaciones para cada componente en el vehículo, y así, asegurar que todos se actualicen y sean compatibles entre sí. En Aptiv's Smart Vehicle Architecture™, el controlador central del vehículo es el maestro. Este enfoque garantiza que el sistema evite una falta de coincidencia cuando, por ejemplo, un componente espera datos en un formato determinado de otro, pero no los recibe porque existe una actualización incompleta o interrumpida.

Más allá de la tecnología OTA, la centralización del software tiene otros beneficios también. Con aplicaciones de software contenidos en una plataforma común, conducir pruebas de interoperabilidad y dedicar ciberseguridad para esas aplicaciones se vuelve mucho más fácil.

Por todas estas razones y más, la centralización sigue ganando terreno en la industria.

MÁS RÁPIDO Y MÁS SEGURO

Para lograr las actualizaciones OTA más seguras y confiables, cada procesador en un controlador de dominio (y los procesadores en sensores, de ser necesarios) debe tener una capacidad de memoria para contener la imagen del software viejo y del nuevo. Solo cuando las imágenes del software nuevo se descargan, descifran y verifican por completo, el sistema cambia y todos los procesadores afectados lo hacen simultáneamente. Esto garantiza que todos los componentes sigan siendo reiniciables en todo momento.

Se han utilizados tres métodos para facilitar las actualizaciones OTA. Cada método es progresivamente más rápido, y más fabricantes están optando por métodos más rápidos para asegurar la seguridad y flexibilidad.

1. **Actualización desde el almacenamiento externo.** En este escenario, las nuevas imágenes de software se almacenan en una puerta de enlace externa que se comunica con la nube a través de un módem celular. Este método es rentable, ya que no necesita memoria adicional en el controlador de dominio ni en los sensores. También permite que cualquier componente actual esté listo para la tecnología OTA. Sin embargo, no existe la posibilidad de volver a las imágenes anteriores si se produce un error. Una actualización típica para un controlador de dominio avanzado del sistema de asistencia al conductor (ADAS) podría demorar hasta 2 minutos.
2. **Actualización desde el almacenamiento local.** En este escenario, las nuevas imágenes de software se descargan al almacenamiento local dentro de la unidad de control electrónico. Un proceso de actualización copia la nueva imagen del almacenamiento local a la memoria flash activa. Utilizar esta técnica para actualizar un sensor de radar, por ejemplo, tomaría alrededor de 14 segundos.
3. **Actualización desde la memoria flash doble.** En este escenario, el procesador contiene suficiente memoria para albergar tanto la imagen de software anterior como la imagen nueva en una configuración A/B. Una vez que se completa y se verifica la descarga, el cambio a la nueva imagen es casi instantáneo. El cambio no afecta la disponibilidad del sistema. Volver a las imágenes anteriores si se produce un error también es instantáneo.

El momento en que sucede todo esto depende de los fabricantes de equipos originales. Un enfoque sería descargar una imagen de software mientras el vehículo se está conduciendo y luego instalar la nueva imagen la próxima vez que se encienda el vehículo. Otro enfoque sería descargar e instalar las actualizaciones cuando el encendido está apagado, quizás durante la noche. Este último método necesita que el sistema esté alimentado durante ese tiempo, por lo que se debe tener en cuenta la gestión de energía.

¿CON QUÉ FRECUENCIA?

La frecuencia con la que una aplicación se actualiza mediante la tecnología OTA también depende de los fabricantes de equipos originales y, probablemente, dependerá del tipo de aplicación.

Por ejemplo, es posible que una característica madura destinada a cumplir con los requisitos de cumplimiento no necesite actualizaciones OTA con mucha frecuencia o en absoluto. Pero una configuración que se centre en las funciones de comodidad podría beneficiarse de actualizaciones más periódicas, y una función premium podría beneficiarse de actualizaciones casi continuas para garantizar que los consumidores tengan las funciones más recientes disponibles en sus vehículos en todo momento. Por supuesto, esto también significa que cualquier corrección de errores se implementará tan pronto como la situación lo exija.

Las actualizaciones frecuentes encajan bien con la práctica de integración continua/ continua (CI/CD), un enfoque de desarrollo y operaciones que comenzó en TI y se está adoptando con rapidez en la industria automotriz. Con CI/CD, los desarrolladores usan herramientas automatizadas para realizar actualizaciones de software con mayor frecuencia y poner esos cambios en el campo tan pronto como estén listos, y la tecnología OTA está evolucionando para permitir eso.

“Para optimizar la tecnología OTA, es clave centralizar el control de cálculos dentro del vehículo, de modo que las actualizaciones solo tengan que descargarse en esa ubicación central, en lugar de distribuirse a los sistemas en todo el vehículo”.



EL FUTURO: ACTUALIZACIONES FRAGMENTADAS

Hoy en día, la mayoría de las actualizaciones OTA necesitan reprogramar una imagen completa. Sin embargo, los sistemas están evolucionando rápidamente para permitir que se actualicen porciones más pequeñas de software sin un intercambio completo de imágenes, así como estamos acostumbrados a que los teléfonos inteligentes permitan actualizaciones de aplicaciones individuales. De hecho, a medida que Android y otros sistemas operativos [pasan a plataformas automotrices](#), ya están comenzando a generar actualizaciones de aplicaciones a través de tecnología OTA.

La necesidad de permitir tales actualizaciones aumenta a medida que crece la cantidad de software en un vehículo. Si bien muchos vehículos hoy en día funcionan en los niveles de conducción automatizada 0 a 2, los niveles 3 y superiores tendrán muchos más programas de software, y actualizar una imagen completa cada vez podría resultar exorbitante.

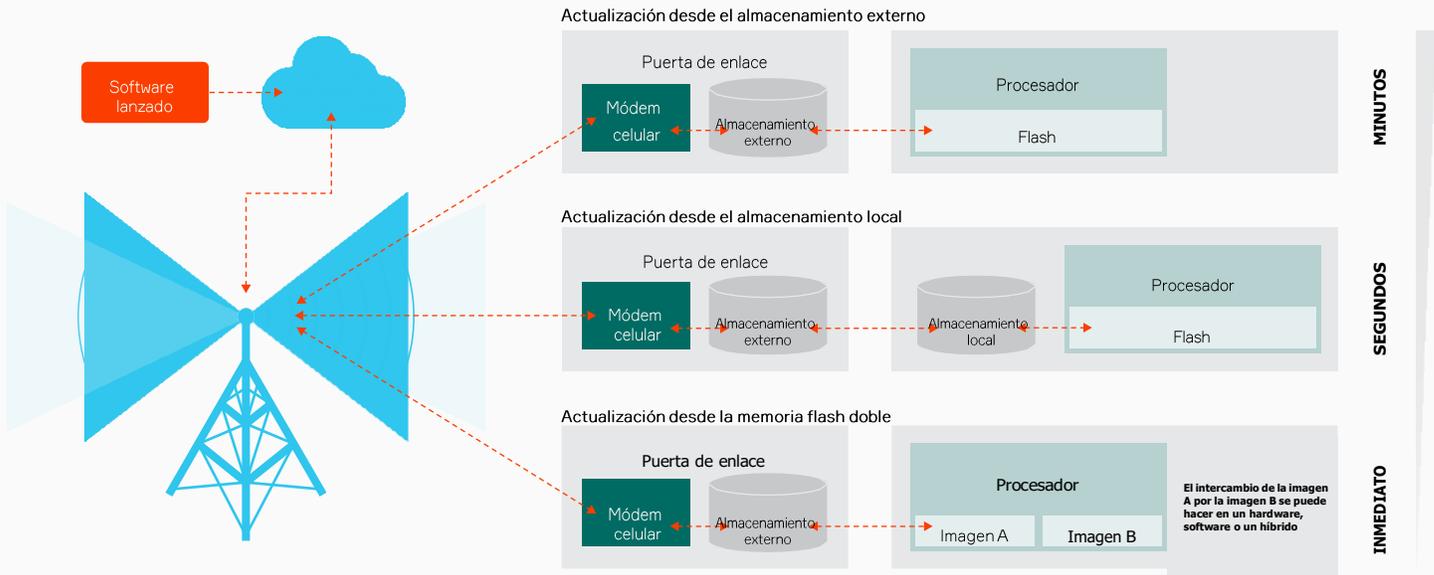
Al mismo tiempo, la creciente funcionalidad definida por el software significa más líneas de códigos y más fuentes que proporcionan piezas del rompecabezas del software. Idealmente, los fabricantes de equipos originales querrían tener la capacidad de actualizar solo la parte del software en un vehículo desde una sola fuente, por ejemplo, el rastreador o la función de control de crucero adaptativo, y dejar las otras piezas intactas. El software dedicado desempaquetaría esas actualizaciones, las colocaría en las ubicaciones relevantes y reiniciaría el sistema. Por este motivo la arquitectura del software es extremadamente importante; debe habilitar la contención que mantiene las piezas separadas y permite estas actualizaciones que se incrementan.

Con cualquier actualización OTA, la seguridad es la principal preocupación en cada paso del proceso. Antes de implementar la actualización, los ingenieros deben analizar el código por completo, no solo para asegurarse de que funcione bien con otro software en el vehículo, sino también para verificar si hay amenazas y vulnerabilidades comunes. Las mejores prácticas se establecen en la norma de ciberseguridad automotriz ISO/SAE 21434, pero esencialmente los mismos sistemas deben diseñarse con una mentalidad de “[inferir daño](#)”, es decir, suponer que cualquier software nuevo podría causar daño, ya sea con intención (si hay un ataque cibernético) o sin ella, y tomar medidas proactivas y reactivas para contener ese daño.

“El éxito del vehículo operado con software depende de la tecnología OTA para la evolución continua de las funciones que los consumidores esperan de otros productos”.

Escenarios de actualización.

A medida que el software se lanza a la nube, los vehículos descargan las actualizaciones al almacenamiento externo centralizado. Desde ese momento, hay varias formas de propagar esas actualizaciones a los procesadores individuales.



NUEVOS MODELOS DE NEGOCIOS

Las posibilidades de mejoras continuas en las características de los vehículos son prometedoras, pero la oportunidad de nuevos modelos comerciales que aprovechan la tecnología OTA es igual de interesante.

Un modelo podría ser el de ofrecer funciones a través de un servicio de suscripción, cobrando por las funciones a través de la facturación recurrente. O un conductor puede querer activar una asistencia de conducción en carretera el tiempo suficiente para una escapada de fin de semana. La tecnología OTA permitiría que las funciones se descarguen o se habiliten solo durante el tiempo en que la suscripción esté activa.

Cuando un vehículo tiene suficiente memoria y capacidad de cómputo, junto con una variedad de radares, cámaras y otros sensores, todo lo que se necesita para las funciones nuevas es el software, que se entrega por medio de tecnología OTA.

La tecnología OTA es una pieza fundamental de cualquier arquitectura eléctrica y electrónica de próxima generación, y Aptiv ha diseñado

el enfoque [Smart Vehicle Architecture™](#) y la [plataforma ADAS de última generación](#) para garantizar que estén optimizados a fin de recibir actualizaciones OTA de la manera más eficiente y segura posible.

El éxito del vehículo operado con software depende de la tecnología OTA para la evolución continua de las funciones que los consumidores esperan de otros productos. La tecnología OTA es una pieza clave para fomentar un ecosistema de proveedores de software, aprovechar su innovación y permitir que esa innovación florezca durante la vida útil de un vehículo.

SOBRE EL AUTOR



Nabeel Bitar

Arquitecto de sistema para vehículos – Advanced Safety Start Center

Nabeel Bitar es responsable de los análisis y diseños técnicos globales de fabricantes de equipos originales para nuevas oportunidades comerciales en seguridad avanzada. Nabeel ha estado en Aptiv por más de 25 años en tareas de ingeniería de software y sistemas y ha estado desarrollando ADAS y sistemas de conducción autónomos desde 2003. Anteriormente, Nabeel diseñó un software de control de tracción y frenos antibloqueo, así como unos sistemas de dirección asistida eléctrica en Delphi Saginaw Steering (ahora Nexteer).

CONOZCA MÁS EN [APTIV.COM/CONNECTIVITY-SECURITY](https://www.aptiv.com/connectivity-security) →