WIND™

Implementing Over-the-Air Software Updates for Automotive Applications

A Look at the Opportunities and Challenges

WHEN IT MATTERS, IT RUNS ON WIND RIVER

EXECUTIVE SUMMARY

It was inevitable that the increasing amount of software installed in a car would one day pose a problem. When you consider the infotainment system, advanced driver assistance system (ADAS), and under-the-hood software used for engine management, you can be sure that it all will need updating at some stage. The need to keep all of this software up to date and secure is challenging the industry. And that's just current functionality—the expectation of new features and functionality is just as important. As Figure 1 illustrates, current projections are that within the coming decade, approximately 50% of a vehicle's value will be defined by software and experiences, compared to just 10% in the past (when the remaining 90% was accounted for by tangible mechanical component parts).

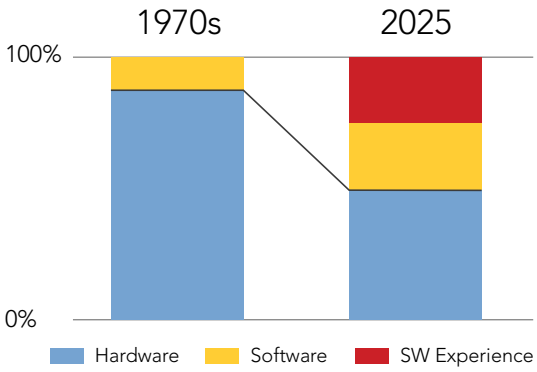

Figure 1. The changing value of automotive, from hardware to software and new applications

Add to the mix the current growth of the Internet of Things (IoT), which demands connection between the vehicle and the outside world, and the challenge becomes significant. As a way of differentiating their vehicle brands and platforms, automakers are keen to add functionality that can enhance the driving experience and raise them above their competitors. Software is making this possible, which means that it is essential to keep the vehicle software environment secure and up to date.

TABLE OF CONTENTS

THE OPPORTUNITY

Among the most critical enablers in this process are over-the-air software and firmware (SOTA/FOTA) updates. Used to manage embedded systems across the lifecycle of the vehicle, from leaving the garage to end of life, these updates provide endless benefits to manufacturers, dealers, and owners. However, just as the opportunities are huge, so too are the challenges, and much still must be learned to make systems reliable, secure, and effective.

During the vehicle development cycle, software updates will need to be managed across a fleet of pre-production vehicles, and usually software is the last thing to be updated prior to the release of a car. The car of today is likely to have a hundred or more control systems or Electronic Control Units (ECUs), and development teams will be faced with several software revision cycles, which could be a versioning nightmare. Add to this the fact that software and systems are often developed across numerous suppliers and several geographically dispersed design centers, and the task of managing software development cycles, versions, and dependencies becomes significant.

Yet even with such challenges, the benefits of OTA, including improved customer experience, significant cost reductions, and opportunity for continuous improvement and new revenue streams through remote access to vehicle data, cannot be ignored.

APPLICATIONS AND USE CASES

According to IHS Markit, it costs automakers up to $100 per software incident for updates applied at the dealership or service bay, not to mention the hours it takes to complete an update, the inconvenience for customers, and the negative impact on brand image. Remote OTA updates will not only save automakers billions of dollars per year on software-related recalls and warranty costs but they will also enable distribution of bug fixes, security patches, and feature improvements and performance enhancements for the lifetime of the vehicle.

With use cases spanning recall automation and just-in-time updates to security countermeasures and continuous improvements, the benefits of OTA will only increase as the industry evolves and the potential of the connected and autonomous car is realized.

One widely deployed use case to date is that of updating consumer-facing maps held within the navigation system. Being able to make updates available without the need for a visit to the dealer premises ensures that the overall navigation experience is trouble-free. New roads, developments, and changing junction/direction priorities can make for a stressful navigation experience. Also, the ability to download maps on request or automatically, for example as the vehicle is traveling across a country or a regional border, further enhances the experience.

Engine management and ADAS-based software can also be updated this way. Many vehicle functions such as steering, braking, and suspension control are now reliant on electronic actuation. With such safety-critical functions, it is imperative that the latest versions of firmware and software are active. Given the associated costs—say hundreds of dollars for a dealer recall—and the pure customer inconvenience, undertaking recalls (potentially on millions of vehicles) due to software problems triggers expenses that could amount to billions of dollars for the OEM. The use of OTA can dramatically reduce these costs and the associated downtime, benefiting both the manufacturer and the vehicle owner.

CONNECTIVITY

Today, OTA is restricted to noncritical applications, such audiovisual infotainment systems. The under-the-hood and safety-critical resources such as brakes, engine control, blind-spot detection, and adaptive cruise control are reserved for updating at the dealership's service center, where the process can be properly controlled and fully tested before handing the vehicle back to the customer. However, as link reliability, bandwidth, and link security improve, so will the range of updatable applications. According to Strategy Analytics, some OEMs aim to update all ECUs in the vehicle across fleets by 2020.

While OTA opens the opportunity to remotely update firmware and software, it also opens the vehicle system to the Internet. The security challenges associated with any connected device arise, along automotive-specific safety and reliability concerns. Consider, as well, connection requirements and cost for OTA enablement. Given varying data rates, automakers must ensure that the connection to the vehicle is robust enough to transmit required updates while keeping costs low. In the face of widely varying bandwidth and signal strengths, the OTA solution must be capable of completing and verifying update downloads that have had to stop and start several times.

Additional concerns for OTA include software update verification, potential impact on other systems within the car, and unauthorized access to vehicle software. In addition, the potential use of OTA may challenge existing elements of the current automotive industry. For example, reducing customer visits to dealerships can have a significant impact on the dealership revenue model.

SECURITY

As mentioned earlier, there are major security implications for enabling OTA updates. When software within and connections to the vehicle increase, so too does the likelihood of software bugs, security breaches, IP theft, and compromised safety. The potential impact of these vulnerabilities reaches beyond single vehicles and vehicle owners, having the ability to compromise entire fleets of vehicles. While less critical hacking attempts could stop or alter infotainment systems or present incorrect positional information, the primary concern is that a breach could present a significant safety risk. There is also the likelihood that private and personal information might be compromised. The data path from vehicle sensor to data center presents many opportunities for intrusions such as man-in-the-middle attacks, so it is important that steps be taken to minimize the risks.

Development of OTA technology and security standards similar to ISO 26262 will serve to speed manufacturer adoption and increase automaker confidence in the quality and robustness of security features from software suppliers.

Beyond the adherence to security and safety standards, OTA update solutions must, at minimum, ensure integrity, confidentiality, availability, and authenticity. This means the following must be ensured:

- Confidentiality of OEM IP and data processed
- OTA update and metadata integrity, preventing attackers from installing malicious firmware in the vehicle
- Availability of vehicle-to-cloud and in-vehicle communication
- Authenticity, integrity, and timeliness of all metadata exchanged between vehicles and the cloud
- Verification of software updates to be installed in the vehicle
- Secure communications and payload data, using symmetric and asymmetric cryptography

WIND RIVER HELIX CHASSIS

To help automakers meet the challenges of the next-generation automotive technology, Wind River® provides its Wind River Helix™ Chassis product line, a software framework for the connected and autonomous car (see Figure 2). Helix Chassis is comprised of three core product offerings: Wind River Helix Cockpit, a software platform for consolidated in-vehicle computing, enabling safe, secure, and seamlessly connected experiences; Wind River Helix Drive, an ISO 26262 certifiable development platform for safety-oriented systems including ADAS and autonomous driving applications; and Wind River Helix Edge Sync for OTA updates and software lifecycle management.

Specifically, Edge Sync enables automakers to remotely and securely maintain the integrity of embedded systems while providing new features and functionality through the entire lifecycle of the vehicle, thereby maintaining a fresh, exciting, safe, and secure driving experience.

While today the benefits of OTA are reserved for high-end luxury vehicles, the development of secure and reliable communication standards and the fine-tuning of the OTA process will help vehicle manufacturers roll out this approach across whole fleets and extend OTA to safety-critical ECUs to provide vehicle performance and functionality improvements.

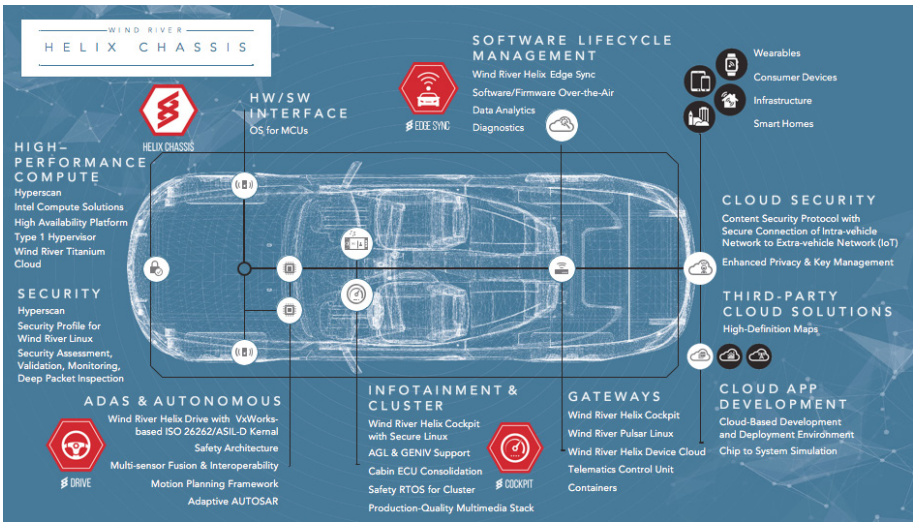

Figure 2. Wind River Helix Chassis automotive development suite, including OTA update and SWLC management via Wind River Helix Edge Sync

Wind River is a global leader in delivering software for the Internet of Things. The company's technology is found in more than 2 billion devices, backed by world-class professional services and customer support. Wind River delivers the software and expertise that enable the innovation and deployment of safe, secure, and reliable intelligent systems.