Updating Car ECUs Over-The-Air (FOTA)

White Paper
ABSTRACT

As the amount of software in automobiles grows, so too does the need to effectively manage that software asset. The telecom industry has a proven solution for remotely updating software on mobile devices. The technology is called Firmware Over-the-Air (FOTA) updating. All major mobile phone manufacturers and tier one operators have adopted FOTA successfully, performing more than 100 million updates per year with the benefit of providing new features and performance improvements, reducing customer care costs, avoiding product recalls, and increasing consumer satisfaction. FOTA technology is now entering the automotive industry. This paper describes the existing update methodology in the automotive industry, its pros and cons, and the benefits of using FOTA in automotive.

1 INTRODUCTION

1.1 Software in Automobiles

Today’s automobile contains many complex electronic systems; each may incorporate a large number of Electronic Control Units (ECUs) performing a single function and communicating via a common bus/network.

In a 2009 article in IEEE Spectrum, Prof. Manfred Broy says that in a premium class automobile there are close to 100 million lines of software codes, compared to the F-35 Joint Strike Fighter with 5.7 million lines or with the Boeing 787 with about 6.5 million lines.

According to the article, Alfred Katzenback, the director of information technology management at Daimler, said that the radio and navigation system in the 2009 S-Class require over 20 million lines of code alone and that the car contains nearly as many ECUs as the new Airbus A380 (excluding the plane’s in-flight entertainment system).

In addition, Prof. Broy states in the article that “the cost of software and electronics can reach 35 to 40 percent of the cost of a car.”

Present day automobiles typically contain more than 60 ECUs such as the audio system, brake system, doors, lighting, engine, transmission, batteries, and more. The embedded software package size is now tens of megabytes for engine and transmission controllers, while audio/infotainment systems are usually the largest and most complicated software units, often exceeding 100MB.

1.2 Warranty Claims

Warranty-claim cost in the automotive industry is very significant and accounts for $1,100 on an average per vehicle in the European Union (Warranty Week, July 7, 2011). In the U.S., the numbers are lower than in the EU and are less than $500 on average.

The total automotive warranty costs for 2010 in the U.S. was close to $4.7B (Warranty Week, September 21, 2011). Warranty Week published figures of warranty claims per several OEMs ranging from 0.9% in Honda (of the Average Selling Price) to 4% in Volkswagen (refer to the figure below).

In an article that was written by Manjunath S (Software in Motion, August 2011), IBM claims that approximately 50 percent of the car warranty costs are now related to electronics and their
Updating Car ECUs Over-The-Air (FOTA)

confidential software, which means that if the automotive industry will use FOTA updating it could provide a significant leap forward towards reducing warranty costs.

Figure 1: Different OEMs and Their Warranty Cost as a Percentage of Product Sales

Figure 2: Japanese Automotive OEMs Product Warranty Accruals 2003-2011 as a % of Automotive Revenue

Note: Toyota and Honda follow a fiscal year running from April 1 to March 31.
2 Embedded Software Update in Automobiles TODAY

There are many control modules in a vehicle, most of which are interconnected over some form of vehicle network interface (CAN, MOST, LIN, FlexRay). However, only a select few will have access to external cellular or Wi-Fi networks, typically the infotainment head unit or Telematics module. It is possible to use an externally connected module as a gateway for updates, where firmware updates for other modules are received by this gateway module and then transferred to the appropriate module over a vehicle network. In any case, each of the vehicle control modules will potentially be subject to updates.

There are several use cases today for updating automobile software:

- Recall (mandatory or voluntary)
- During scheduled maintenance
- Customer complaint
- Delivering new features and applications

The recall case is the most common, and involves the following process:

1. A vehicle manufacturer finds a problem with the vehicle functionality. The affected functionality can be fixed by changing software in one of the vehicle’s ECUs.
2. The appropriate ECU supplier is requested to provide a new release. The supplier ships the software release to the Original Equipment Manufacturer (OEM), which tests it for quality assurance (QA).
3. The OEM notifies the dealers and owners of the recall via mail. The OEM sends the new software version to the dealers on a CD by mail as well. The dealer updates the reprogramming (serial communication) tools with the content from the CD.
4. The vehicle owner drops off the vehicle at the dealer shop and registers at the front desk.
5. The technician connects a serial communication tool to the in-vehicle bus to access the targeted ECU.
6. The technician starts the update process of the targeted ECU.
7. The technician checks the targeted ECU for the new software version to make sure proper re-flashing happened.
8. The customer picks up the updated vehicle.
9. The dealer charges the OEM for the recall labor.

The update duration changes significantly depending on the module size and the speed of the serial protocol; however due to a lot of overhead, dealers are charging 1-2 hours of labor for such activity. There are some car models where the update can take more than 2 hours. It should be noted that programming tools are rather expensive, so there is a limit to the number of simultaneous re-programming.
2.1 Assessment of the Current Reprogramming (Cable-Based) Method

There are limitations and constraints with current software distribution and software update processes:

- Any update is distributed to all dealers. This takes time and resources. It may also cause delays in getting the latest software to the vehicles. In addition, all dealers need to maintain a software version library, which consumes resources.
- The download process and the manual setup take a long time, resulting in higher cost of labor, inconvenience, and customer dissatisfaction. Due to this long duration, the consumer needs to drop off the vehicle and return later to pick it up – a major inconvenience.
- The process cannot be scaled or performed in parallel, as it involves a physical equipment connection.
- Some existing re-flashing methods require sequential updates, meaning from version 1 to 2 to 3, which can make the entire update process longer.
- Sometimes (for off-highway vehicles), the re-flashing equipment needs to be mobilized to the vehicle.
- It may take a long time from when the customer is notified to the time the vehicle is actually updated. Many customers do not respond to recall notices. For older vehicles, the OEM may not have the latest vehicle owner information, meaning some vehicles never receive needed updates. Conducting a successful recall depends on the customer cooperation.
- Reprogramming of the ECU is performed manually.
- The customer becomes aware of the problem and overall customer satisfaction decreases.

There are some advantages to the current reprogramming (cable-based) method:

- While FOTA is gaining wide acceptance for new automotive platforms, it will take few years until FOTA is a widely adopted solution in the automotive industry.
- Reprogramming is performed in the controlled environment.
- The vehicle is not moving and it is under technician supervision while the reprogramming occurs.
- This methodology is proven and it has worked in the past.
- Any problem that occurs has more chances to be detected immediately by a trained technician.
- Vehicle wired serial communication protocols and algorithms for reprogramming are proprietary and closed source by nature. As such, protocols provide an added layer of security against unauthorized software changes.
3 Firmware Over-The-Air (FOTA) Update Technology

The FOTA update process comprises three primary stages: generating the update, managing the delivery of the update, and performing the update.

Figure 1: Typical FOTA Solution High-Level Architecture

3.1 Generating the Update Package

To perform a FOTA update, a software update package containing defect fixes or new features must be generated. In order to make this package as small as possible (in general it is less than 5% of the original size), the update package includes only the changes (also referred to as the “delta”) between the version that already exists on the ECU and the new version being deployed to the vehicle. This update package is typically generated by the owner of the software, most often a tier I vendor.

3.2 Managing the Delivery of the Update Package

Once generated, the update package is published to a distribution platform. In the mobile industry, this platform is managed by either the mobile phone manufacturer or the network operator. In automotive, this platform is managed by the OEM. This platform manages the various versions of the update packages and handles the actual network delivery (download) of the packages to the appropriate vehicle model and specific ECU. There are typically multiple versions of update packages, each intended for particular vehicle models and configurations. This portion of the process can be an integral part of an overall Telematics or over-the-air (OTA) diagnostics system.

A centralized software package repository is used for the FOTA use cases, which are described below. This centralized repository replaces the distribution of software updates to the various dealers. It significantly reduces the Time-To-Market (TTM) of any new software version. This system is also responsible for the delta package delivery to the device. There are several ways to perform such a delivery. In mobile, most market players use a standard protocol developed through the Open Mobile Alliance Device Management (OMA-DM) organization.
3.3 Performing the Update

In this third stage of the process, the downloaded update package is used to perform the actual update (re-flashing) of the original software image. The update package and the FOTA update software necessary to perform the update occupy a small amount of memory allocated within the embedded device in the vehicle (to address the challenges associated with the limited memory resources). In this stage, the FOTA update software validates that the correct update package has been received and that the update process has been successfully completed. It is important to mention that the FOTA updates do not need to be sequential and can support any-to-any software version update.
### 4 FOTA - Changing the ECU Update Paradigm

The current method of updating software in cars was suitable when the amount of software was minimal. Now that software has become vital to the operation and feature-set of cars, the method of software updating must be improved.

It is clear that performing the update in the customer location and not in the dealership represents a better and more optimized method in term of cost savings and user experience. However, it can introduce some potential procedure challenges such as how to make sure that the car will not be driven in the middle of the update. Therefore, FOTA adoption in the automotive industry will take more time to become fully operational.

#### 4.1 Dealership FOTA Scenario

This section describes the OTA dealership use case. The FOTA operation when customers are staying at home is described in the next subsection. Initially, the “Dealership FOTA” use case may be adopted more quickly as it addresses the reliability and liability concerns of the OEMs. Once FOTA updates are performed more frequently, other use cases, much more cost effective, could be implemented.

The use case description is as follows:

1. A vehicle manufacturer finds a problem with the vehicle functionality. The affected functionality can be fixed by modifying the software in one of the vehicle’s ECUs.
2. The appropriate vendor is requested to provide a new delta release. The vendor ships the delta release to the OEM.
3. The OEM notifies the dealers and owners of the recall via mail. The OEM may send the new version to the dealers using a CD by mail as well as electronically.
4. The vehicle owner drops off the vehicles at the dealer shop and registers at the front desk.
5. The technician requests a software update via FOTA to be immediately initiated with the specified vehicle. The main server authenticates against the vehicle and confirms process start.
6. The FOTA process is executed over-the-air (OTA); the delta file is downloaded and updated. A completion status is provided once the process is done (the whole process lasts less than 15 minutes).
7. The vehicle is checked to make sure proper re-flashing happened.
8. Customer picks up the vehicle.
9. The dealer charges the OEM for labor, probably 30 minutes for software operation and checkup.
Some notes to the above process:

- Since the software is maintained centrally by the OEM, the dealers do not need to spend time on storing and managing new updates.
- The process can be executed simultaneously to many cars (10-50), so the limitation of a programming tool is not a bottleneck.
- The vehicle does not need to be positioned inside the garage. It can be parked outside. This saves a lot of time and allows the scale of the process beyond the garage vehicle capacity. In addition, the vehicle owner may not have to leave the dealership at all.
- In case of a power failure, the process restarts from the last written block, saving a lot of time of re-flashing blocks that were already written.
- In some instances, this update might simply involve swap out of the ECU hardware module.

4.2 FOTA at the Customer Location Scenario

This section describes the use case of performing FOTA updates at the customer location. This provides the customer with maximum convenience and OEM cost savings will be maximized.

The use case description is as follows:

1. A vehicle manufacturer finds a problem with the vehicle functionality. The affected functionality can be fixed by changing software in one of the vehicle’s ECUs.
2. The appropriate vendor is requested to provide a new delta release. The vendor ships the delta release to the OEM.
3. The OEM notifies the dealers and owners of the recall via mail. The OEM does not send the new version to the dealers, since the centralized system is used to store all software versions.
4. The vehicle owner calls the dealer and requests a FOTA update. The dealer requests that the owner will keep the car parked (home or office).
5. The technician requests a remote software update (FOTA) process to be immediately initiated with the specified vehicle. The main server authenticates itself with the vehicle and confirms the process start.
6. The FOTA process is executed OTA (the delta file is downloaded and updated). A completion status is provided once the process is done (usually less than 15 minutes).
7. The owner is notified to perform a check on his/her vehicle to make sure it is operational.
8. The dealer charges the OEM for labor (probably 15 min for software operation and vehicle checkup).
9. This process could be implemented using an Interactive Voice Response (IVR) to save costs.
Some notes to the above process:

- The software update packages are maintained centrally by the OEM so the dealer does not need to spend time on storing new updates.
- The process can be executed simultaneously to many cars (hundreds and thousands), so the limitation of a programming tool is not a bottleneck.
- The vehicle is located at the customer location, so the dealer garage parking space does not pose any limitation.
- The OEM can use an Interactive Voice Response (IVR) utility to further scale the process and save on labor.

### 4.3 Incentives to Using FOTA for Automotive

There are many incentives to use FOTA in automotive, including the following:

- Warranty cost reduction – recall cost will go down. The technicians’ and customers’ time is saved.
- Location independent – wireless communication can provide a method for vehicles to be updated without requiring their physical presence at the dealer.
- Shorter correction cycle – product as well as software development is subject to rigorous developmental processes, tests, and reviews. Re-flashing existing ECUs in the field adds to the quality of the product.
- Centralized server – all updates are located in a centralized server and are not distributed to thousands of dealers. This saves potential errors and ensures that the latest software is installed. In addition, it reduces the Time-To-Market (TTM) for new software updates.
- Convenience – consumer convenience is already achieved using the dealership FOTA model. When the FOTA is performed at the consumer location, convenience is maximized.
- Allows for forced updates – in some cases, re-programming could be done regardless of customer willingness to cooperate (such as safety related recalls).
- Improves safety – applying wireless software updates decreases the time the recalled vehicle is driven under faulty conditions.
- Proven technology – FOTA is a proven technology used in the telecom industry on more than 1 billion mobile phones and connected wireless devices. In addition, cellular service inside automobiles is very robust and available, so there should be no issue in coverage and reception.
- There is no need to have a fully trained technician to perform the update.

### 4.4 Granularity of Updates and User Involvement

In general, in a given module there may be a variety of software components that are independently updatable. Using a modern infotainment system as an example, these might include a base firmware image, a navigation system, a music/multimedia database, voice recognition system, and other upgradable software components. Some updates might be considered mandatory, while others may be provided on-demand or with user approval. A quiet update might be preferred for mandatory “push” updates, while a more user-engaging approach will be preferred for elective updates or those that require end-user approval.
In an extreme case, a user-directed update might contain entirely new features and applications, as typically made available through an App Store. In this case, an inventory of available content is provided to the user, from which new features can be selected. The same FOTA update mechanisms can be engaged to facilitate such an update.

4.5 Other Use Cases for Performing FOTA

There are three areas where FOTA is already in production cars:

- In-Vehicle Infotainment (IVI)
- Electrical Vehicle (EV)
- Telematics Units

There are several reasons why car manufactures and tier 1 OEMs have decided to implement FOTA in these automotive systems. The frequent number of changes to the component code requires using new and proven methods for doing over the air updates. In addition, using FOTA with the ability to send over-the-air only the changes between the versions allows car manufactures and service providers to reduce costs by saving cellular and roaming expenses.
5 FOTA Considerations

Most of the considerations which are described below are already addressed by the telecom industry, and the automotive industry could leverage these proven standards and protocols.

5.1 Technical Considerations

- **Download protocol** – a method needs to be implemented to securely and reliably transfer software packages wirelessly from the vehicle manufacturer to the targeted vehicles’ ECUs. The telecom OMA-DM standard provides a viable option for automotive.

- **Outside/cellular channel** – at least one wireless-capable component needs to act as a wireless gateway and must be connected with the other embedded systems using internal buses or Bluetooth.

- **Multiple devices** – in the vehicle there are multiple devices that need to be updated. It does not make economic sense that each one of them will have an external wireless channel for updating. The same gateway concept described above could be used.

- **The ability to support multiple communication protocols such as cellular and Wi-Fi.**

- **The re-flashing process should be considered when calculating the battery lifetime.**

- **The vehicle needs to be in a wireless reception area in order to download the new software version over the air.**

- **It is possible to separate the download process from the update process so that the update process can be performed even in areas without wireless reception.**

- **The storage will slightly increase to store the delta and the update agent.**

- **The FOTA updating system must be capable of updating both the Read/Write and the Write-only area in the memory.**

- **The FOTA updating system must minimize the download and the update time.**

5.2 Customer and Process Considerations

Updating software that will alter vehicle functionality without consent may upset the customer. The customer may notice a change in the vehicle functionality that will lead him/her to think that there is a problem in the vehicle. A customer needs to be informed of the software update. A good example is a display on the instrument panel indicating that a software update occurred. The display could show software change identification (SCID). A customer can then log on to the vehicle manufacturer’s website and look up the SCID to find out more information about the software change.

The FOTA updating system must be able to intelligently decide which wireless technology to use based on the location of the vehicle. For example, when the car is parked at home, the FOTA update may be performed over Wi-Fi and not cellular.

The industry must establish procedures for when to perform the update. For example, processes and safeguards must be put in place so that ECUs are not updated while they are performing a vehicle function, and only when the vehicle is not moving and the ignition key is set to the off position.
5.3 Dealer Issues

The dealers will lose a significant revenue source with the reduction of maintenance labor required for software updates.

In the beginning, the process will not be ubiquitous, since not all systems could have OTA updates. This may be a source for confusion.

5.4 Vehicle Manufacturer (OEM) Considerations

The vehicle manufacturer must keep track of each individual vehicle’s ECUs and software releases including the dependency between the ECUs. The list must be updated when a particular ECU software is updated.

Developing the right testing and validation process, the vehicle must operate properly after the software update. Under no circumstances the updating process should affect safety of the passengers’ integrity of the software after re-flashing in the targeted ECU must be guaranteed.

Building the back-end infrastructure that will be responsible for sending the updates over the air to the cars. In some cases, this infrastructure should be connected to other systems, such as customer care or billing, since it can be used also as the delivery system for the application store.
6 Summary

The car industry is going through the same trend that the mobile industry experienced eight years ago, where the need to maintain the increasing amount of software is forcing the industry to look for new, more efficient, and more cost-effective methods. Updating car ECUs has become a mandatory operation. The current mode of doing an update is costly, not customer friendly, and not flexible enough to cope with the rapid changes that are happening in the car industry.

FOTA technology is a proven, safe, and cost-effective method for OEMs and car manufactures to manage the car software evolution, which is turning the car from iron driven to code driven. FOTA can help auto makers to save time and costs, mitigate risk, and attract and retain customers. In addition, this can enable car manufactures to establish new ways of up-selling services and deliver new features and applications to consumers throughout the car lifecycle.

Changing the existing update methodology to FOTA should be gradually performed. With the experience and lessons learned in the telecom industry, this migration can be smooth and successful for the automotive industry.