Transmitted by the expert from ITU

Document No. ITS/AD-08-09
(8th ITS/AD, 9 March 2016, agenda item 4)

Secure Over-the-Air Vehicle Software Updates

Operational and Functional Requirements

Revised 24 February 2016

Author contact:

Michael L. Sena Consulting AB
Sundbyvägen 38
SE-64551 Strängnäs
Sweden
Phone: +46 733 961 341
Fax: +46 152 155 00
Email: **ml.sena@mlscab.se**
www.michaellsena.com

Table of Contents

Secure OTA Vehicle Software Updates

Operation and Functional Requirements

1. Introduction

1.1. Executive Summary

A vehicle exists in many different states from the time it is assembled in a factory until it is disassembled and recycled. It is therefore essential that the entire life-cycle of a vehicle is considered when developing a technical solution to secure over-the-air updating of a vehicle's electronic control units, software or data storage devices. Secure in this context means providing protection from unlawful, undesirable and unqualified intervention in, or access to, vehicle systems. Properly designed Internet- and cellular-connected on-board devices are the crucial starting points. A well-designed over-the-air telecommunications method is vital for achieving the highest level of security. Proven techniques and technologies exist for designing secure on-board systems and for delivering firmware over-the-air (FOTA) and software over-the-air (SOTA) updates to vehicles, and these are the focus of intensive standardisation efforts at this time.

This document addresses the business process issues of secure over-the-air updating. FOTA/SOTA telecommunications standardisation must be complemented by a set of business methods that on one hand are comprehensive enough to cover the full life-cycle of all vehicles and on the other can accommodate the individual practices of the vehicle OEMs from the time a vehicle is designed until it is taken out of service. This document identifies and clarifies the business process issues that must function in parallel to the technical ones.

1.2. Objectives

The principal objective of this document is to provide supportive information to the groups working on the technical specifications for a FOTA/SOTA telecommunications standard.

A secondary objective of this document is to provide background information to the vehicle OEM groups working on their internal processes aimed at delivering an OEM-specific end-to-end FOTA/SOTA update solution for their own vehicles. By having a common understanding among all vehicle OEMs of the requirements for the complete end-to-end process, it should be easier to create a technical specification standard that delivers a secure update while allowing for the differences among the OEMs.

1.3. References

- Secure Software Update for ITS Communications Devices in ITU-T Standardization; Koji Nakao, Research Executive Director, Cybersecurity Research Center, Network Security Research Institute, NICT, Japan.
- Esworthy, Robert, Specialist in Environmental Policy – Federal Pollution Control Laws: How Are They Enforced? Congressional Research Service (October 7, 2014).
- Canis, Bill and Lattanzio, Richard K. – U.S. and EU Motor Vehicle Standards:

Issues for Transatlantic Trade Negotiations (February 18, 2014).

1.4. Acronyms and Definitions

Term	Definition
Authorized Driver	The physical or legal person who is insured to operate the vehicle, or who is driving the vehicle on the insured's order or with the insured's permission. The person responsible for the vehicle so far as official communications from the police or other authorities. Also known as 'registered keep' in certain jurisdictions. (See Registered Owner)
Complete Vehicle	Means any vehicle which has been built in one stage by one manufacturer, for example a panel van.
Conformity of Production Certificate (COP)	Means a document issued to a manufacturer after an assessment, carried out by the approval body, of production processes and systems â€" to certify that they conform to the required quality specification.
Conformity of Compliance Certificate (COC)	Means a document which is issued by a manufacturer, certifying that a vehicle has been produced under the same production processes and systems as an example of the type which has achieved Type Approval.
Cybersecurity	The protection of information systems from theft or damage to the hardware, the software, and to the information on them, as well as from disruption or misdirection of the services they provide.[
DTC	Diagnostic Trouble Code – The standardized codes received from the OBD-II port.
EC Type Approval	Means the procedure whereby an authority of an EU member state certifies that a type of vehicle, system, component or separate technical unit satisfies relevant technical requirements and administrative provisions listed in the Directive.
ECU	Electronic Control Unit is a generic term for any embedded system that controls one or more of the electrical systems or subsystems in a motor vehicle. The ECU involves both hardware and software required to perform the functions expected from the unit.
Firmware	In electronic systems and computing, firmware is a type of software that provides control, monitoring and data manipulation of engineered products and systems. Typical examples of devices containing firmware are embedded systems (such as traffic lights, consumer appliances, and digital watches), computers, computer peripherals, mobile phones, and digital cameras. The firmware contained in these devices provides the low-level control program for the device. As of 2013, most firmware can be updated.
FOTA	Firmware Over-the-Air

FOTA Update	Updating firmware over-the-air. Firmware is held in non-volatile memory devices such as ROM, EPROM, or flash memory. Some firmware memory devices are permanently installed and cannot be changed after manufacture. Common reasons for updating firmware include fixing bugs or adding features to the device. This may require ROM integrated circuits to be physically replaced, or flash memory to be reprogrammed through a special procedure. Firmware such as the ROM BIOS of a personal computer may contain only elementary basic functions of a device and may only provide services to higher-level software. Firmware such as the program of an embedded system may be the only program that will run on the system and provide all of its functions.
Functional Safety	The detection of a potentially dangerous condition resulting in the activation of a protective or corrective device or mechanism to prevent hazardous events arising or providing mitigation to reduce the fight consequence of the hazardous event. http://www.iec.ch/functionalsafety/explained/
Head Unit	The control centre and user interface for an automobile's entertainment centre, which typically resides in the centre of the dashboard. It provides the main controls for the radios (any combination of AM, FM, XM, Sirius, HD Radio) as well as a CD/DVD player, GPS navigation, Bluetooth cell phone integration, hard disk storage for music and iPod connector. There may be auxiliary controls on the steering wheel.
ICT	Information & Communication Technology
IPR	Intellectual Propriety Rights
IT	Information Technology
ITS	Intelligent Transport System
M2M	Machine-to-Machine
New Type	When looking at application dates within the legislation there will be a reference to 'New Types'. After this date, vehicles of a 'New Type' will be required to meet the legislation in question. A 'New Type' is a vehicle that differs in certain essential respects to a type previously approved or on sale in any market.
OBD-II	On-board Diagnostics, version two. A vehicle's self-diagnostic and reporting system which uses a standardized digital communications port to provide real-time data and a standardized series of diagnostic trouble codes.
OTA	Over-the-Air
OTAMG	OTA Management Group – A group that has the responsibility for an OEM to manage the end-to-end process for FOTA and SOTA.
Registered Owner	The person or the legally accountable entity by whom the vehicle is to be kept (i.e., the person who will be responsible for the use of that vehicle on a day-to-day basis, or, If a vehicle is the subject of a hire-purchase agreement or a lease, the person or the legally accountable entity in possession of the vehicle under the agreement or lease.
SLA	Service Level Agreement

SOTA	Software Over-the-Air update
TCU	Telematics Control Unit
Type	Vehicles of a particular category, which do not differ in certain essential respects set out in Annex II of the framework Directive 2007/46/EC, as amended.
Vehicle Category	Refers to the different forms of vehicles affected by the ECWVTA Directive. These are passenger vehicles (M), goods vehicles (N) and trailers (O), and their sub-divisions.
Wi-Fi	The standard wireless local area network (WLAN) technology for connecting computers and electronic devices to each other and to the Internet. Every laptop, tablet and smartphone comes with Wi-Fi. Wi-Fi is an IEEE standard with the official designation of 802.11. In the early 2000s, 802.11b was the first popular version, followed by 11a, 11g and 11n. The latest is 11ac (see 802.11ac).

2. The Automotive Context

2.1. Are we ready for OTA Updates?

During the past twenty-five years, computer-based electronic control units (ECUs) have gradually replaced many of the mechanical and pneumatic control systems in vehicles. A 2013 study released by Frost & Sullivan found that mass market cars by then had at least 20 million to 30 million lines of software code, while premium cars could have as much as 100 million lines controlling essential systems. According to Frost & Sullivan, the average cost of the software code is $10 per line and it is steadily increasing. They estimate that by 2020 the amount of software will increase by as much as 50 percent.

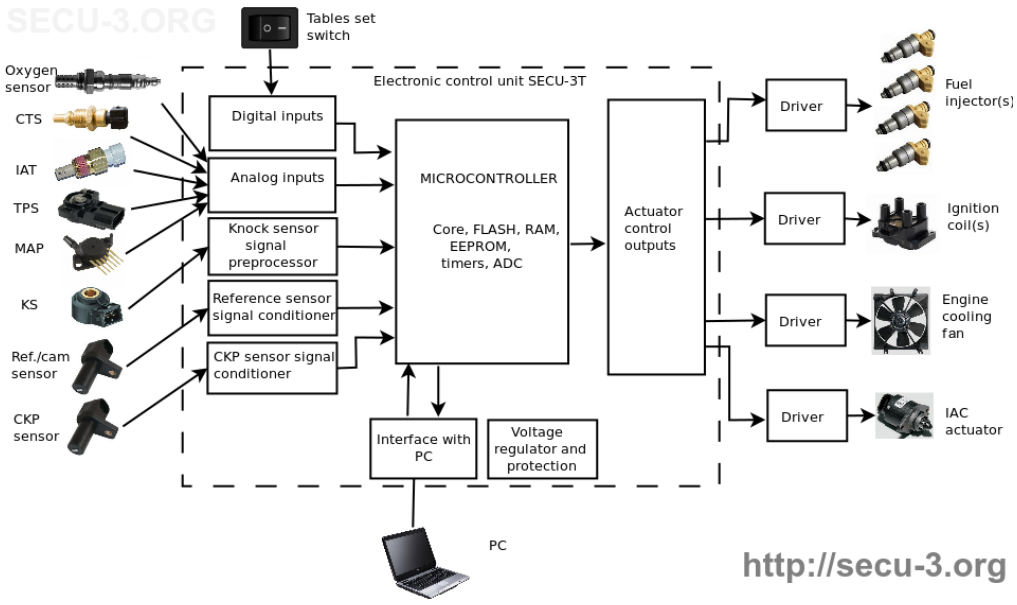


Figure 1: SECU-3 is an internal combustion engine control unit. The microcontroller in the ECU accepts inputs from the various sensors in the vehicle and produces outputs for the drivers of other vehicle systems and sub-systems. Programming and re-programming occurs via an external PC.

It is crucial for vehicle OEMs to manage the software efficiently over the lifecycle of the vehicle, both to provide improvements in performance and to deliver corrections to faulty software that endanger lives or the environment and which could result in expensive product recalls. It is estimated that between 60 and 70 per cent of vehicle recalls in North America and Europe today are due to software problems, so this issue is clearly one that must be addressed aggressively by the OEMs. A topical case in point is Volkswagen and the eleven million diesel vehicles it has sold during the past eight years with 'faulty' emissions control software. A portion of these vehicles also require hardware changes, but if VW could have corrected the problem with only a software update, the process would have taken far less time, cost much less and reduced the environmental impact.

The development of an ECU involves both hardware and software required to perform the functions expected from that particular module. Most automotive

ECU's are being developed today following the V-model.[1] Recently the trend is to dedicate a significant amount of time and effort to develop safe modules by following standards like ISO 26262.[2] It is rare that a module is developed fully from scratch. The design is generally iterative and improvements are made to both the hardware and software. The standard ISO 26262 is an adaptation of the Functional Safety standard IEC 61508 for Automotive Electric/Electronic Systems. ISO 26262 defines functional safety for automotive equipment applicable throughout the lifecycle of all automotive electronic and electrical safety-related systems.

The development of most ECUs is carried out by Tier 1 suppliers based on specifications provided by the OEM. Functional safety features form an integral part of each automotive product development phase, ranging from the specification, to design, implementation, integration, verification, validation, and production release.

Since the introduction of computer-based ECUs, the process used for updating the software in these ECUs once they have been delivered to dealers or to customers has been to connect the vehicle to a vehicle workshop system at an authorized workshop. These vehicle workshop systems, provided by the respective manufacturers of the vehicles to their own workshops, and to independent workshops that have licensed the systems[3], have the means to securely download the required software and to ensure that the component that is operated by this software is fully functional. The contact point for the workshop systems is the on-board diagnostic (OBD) port, and the software download is either made via a physical computer-to-vehicle connection or via a local area network connection from a workshop computer to a wireless device attached to the OBD port.

Connected Vehicles Make OTA Possible

In parallel to the expanded use of ECUs, increasing numbers of vehicle OEMs have gradually incorporated two-way communications devices[4] in their vehicles. Initially, these devices provided safety and security services, such as assistance in the case of a crash or tracking of the vehicle in case it was stolen. They used the mobile network (AMPS, CDMA, GSM) and delivered both voice and data. Most connected vehicle systems today provide both Internet and cellular services. Each OEM, along with its hardware, mobile network operator and connectivity services provider, has taken its own approach to the development of a system and service infrastructure. Early attempts to standardize an over-the-air messaging protocol resulted in limited acceptance by only two OEMs, BMW and Volvo.

There are currently no common standards or industry practices for how an on-

---

[1] National Instruments White Paper on Electronic Control Units.

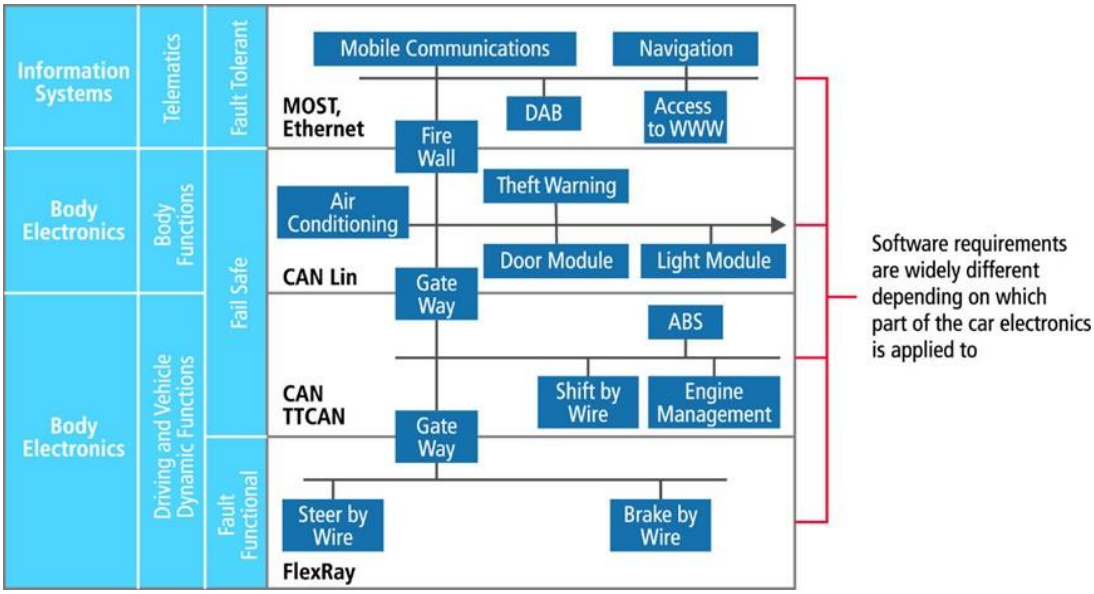
[2] A Functional Safety standard titled “Road vehicle – Functional Safety”. The standard relates to the functional safety of Electrical and Electronic systems, not to that of systems as a whole or of their mechanical subsystems.

[3] In the EU, since June 19, 2011, the automobile industry has been subject to EU Regulation 566/2011 which obligates manufacturers to release electronic data enabling the exact identification of replacement parts for vehicles. This provides independent service providers with the same access to electronic repair and diagnostic information available to OEM authorized repair shops. This regulation does not, however, apply to recall repairs that are provided by the OEM at no cost to the customer, either for parts or labor.

[4] General Motors was first with its OnStar system in 1996. The systems and services have been referred to as ‘telematics’ (remote acting). Connected Cars is the current term.

board system should be designed to achieve the highest level of security for both safety and security services and the broader range of infotainment services. What is known by all OEMs is that security of their on-board connected vehicle systems can be breached, and the consequences can be dire. A properly designed system that provides for as high a level of security as is possible must protect each of the four levels of vehicle electronics systems that could be addressed by OTA software updates:

- Information and entertainment systems
- Fail safe body function systems
- Fail safe driving and vehicle dynamic function systems
- Fault functional driving and vehicle dynamic function systems



Over-the-air updating is already in use among some vehicle OEMs (e.g. Tesla and Mercedes-Benz) as an alternative to performing the software updates using a vehicle workshop system. However, this practice is still very new and limited. A reason why it is not more widespread is the lack of security of the systems. Tesla, which uses OTA extensively, has been shown to have severe security leaks[5]. A Jeep[6] was totally taken over by two researchers and driven off the road.

In a future OTA scenario, whether the updates are performed in the workshop or at the dealer with OTA technology, or remotely, there remain both technical and business reasons for using the dealer network for performing the updates. Unlike a company like Tesla Motors, which sells cars directly to customers and which does not have a dealer network, vehicle OEMs are dependent on their dealers and National Sales Companies for customer contact information.

[5] https://www.google.ch/?gfe_rd=cr&ei=EIdlVv7TBemX8Qfts7CgBw&gws_rd=ssl#q=Tesla+Model+S+Marc+Rogers%2C+cloudflare

[6] Two researchers were able to successfully break through whatever security shields Fiat Chrysler Automobiles and Sprint set up around its UConnect on-board systems and wireless network to take control over the most mission critical functions of a Jeep Cherokee. Starting with the climate controls, the radio and the windshield wipers, the attackers moved to the transmission and the brakes. Eventually, the car was brought to a standstill on a major artery in St. Louis, Missouri in the US. The driver of the vehicle, Andy Greenberg, a journalist with Wired Magazine, was a willing victim, but his description of his experience in Wired indicated that he was truly frightened while he sat helpless in the vehicle while it was being controlled remotely from ten miles away.

Many, if not most, vehicle OEMs do not have a central database containing the names and most recent contact information on the owners or drivers of their vehicles. Dealers with workshops want to continue to have the direct relationships with customers in order to sell service and accessories, and to eventually sell the customer a new vehicle. They will resist any attempt to short circuit them.

Balancing the dealer interests on one side are customer demands on the other side for greater convenience and lower cost of ownership. Constant notices that a vehicle must be returned to the dealer for repair—which, as stated, principally involves updating software—will not be tolerated. The public is aware that their phones and computer devices are capable of being updated with new features and 'bugs' being fixed by quick and efficient over-the-air updating. They will expect the same with the vehicles.

Why OTA?

To lower costs and increase customer satisfaction, vehicle OEMs will want to use OTA for both performance improvements and fault corrections, including both official recalls and non-recalls. Regulators are interested in correcting faults as quickly as possible that are of a level of severity to require a recall. An eventual standard for secure over-the-air updates must absolutely address the fault correction issue, but one that covered performance improvements as well would be of the greatest value to all parties. The current recall process, and even the current process used for informing customers of new features, relies on physical mail and/or electronic mail being sent to a customer. There are numerous problems with this method of contact because mailing lists quickly become out of date. People move without updating their physical addresses, and change e-mail addresses without leaving a trace from their old to new address.

The alternative to trying to make contact with the owner is to make direct contact with the vehicle. This is what Tesla Motors does. It sends a message to the vehicle stating that an update is needed, how long it will take, what to do and what not to do while the update is taking place. This information is displayed on the vehicle's large screen display. Tesla is an example of a company that developed its vehicle from the outset with the intention of having it constantly connected in order to provide important information to the driver about the performance of the vehicle, where the nearest charging station is located, and, importantly, since Tesla does not sell through dealers, when any type of service is needed. Tesla owners are made fully aware of the importance of this feature and commit to use it. Unlike its competitors, since Tesla sells directly to its buyers, it knows exactly who they are and how to contact them.

Sending a message to the vehicle has its own set of issues, including ensuring that the message is received, that it is received by the person who is authorized

to take the action required and that there is a way to maximize the security of communications among the entity sending the update, the authorized owner or registered driver and the vehicle receiving the update.

If OTA were performed using an embedded communications device over the cellular network, it would be the mobile network operator who provides the SIM in GSM solutions—and the equivalent in CDMA solutions—that would have the most reliable information about the vital links in the chain: the location and status of the communications device, and the SIM's IMSI and the MSISDNs associated with it. The mobile network operator is in the optimum position to monitor the flow of data from the server where the updated software is sent to the mobile station in the vehicle. From the time the data enters the vehicle until it is applied to the appropriate ECUs, it would be the responsibility of the vehicle OEM and its tier one suppliers to ensure the proper flow and application of the update. However, the confirmation of successful completion would have to pass back through the network.

Balancing the approach of using the cellular network provider for the highest level of certainty of reaching the greatest number of devices are the needs to keep the costs of transmission as low as possible, to provide a continuous connection to the vehicle for as long as is required to successfully complete the update and to achieve the highest level of security. For the lowest cost, a Wi-Fi connection with today's technology would probably be the optimum solution. For ensuring that the update is completed, which can take from a few minutes to a several hours, an external power source would provide the greatest reliability that the battery is not drained. For security, a closed connection to the vehicle, versus an open IP connection, would be preferred.

There are different conditions that must be satisfied compared with using the mobile network, and these will be identified in this report. Concerning technology, including the use of 4G, which is already in use by many vehicle OEMs to achieve the highest data throughput for infotainment, or 5G which will most likely be ready by the time standards need to finalized, these issues are out of the scope of this report.

In summary, in order for an over-the-air software update standard to be useful and accepted, it must meet the following conditions:

- It must address the entire end-to-end life-cycle processes for the vehicle and its electronics systems.
- It must use the most secure and cost-effective method for performing the updates. It is not simply a matter of defining a protocol or delivering confirmation of completion.
- The standard must address the design of the embedded system, including how the system is activated and provisioned with its contact logic, and how it interfaces with the mobile network or other networks, such as Wi-Fi.
- It must address what to do when a system should perform as if it has been de-activated (e.g. if the customer does not wish to have an actively connected vehicle).
- The design of the system must also conform to the regulations of

privacy that are in effect in the jurisdiction where the vehicle is located when the update is performed.

- Above all, the updating process should be done in complete alignment with the safety and environmental regulations that are in effect in each of the jurisdictions where the vehicles are sold.

2.2. Use Cases

The traditional process for updating ECUs, in which the vehicle owner must take the vehicle to an authorized workshop to have the update performed, varies with the type of update that needs to be performed and how the vehicle owner is informed about the potential update. In the case of a recall, the vehicle owner must be informed by registered mail in the US. In Europe, the use of registered mail varies by country. In addition, the OEM must provide the authorities with a status report on how many of the total vehicles involved in the recall have been updated. For non-recall updates, the vehicle owner either may be made aware of an update via a print or Internet campaign, or informed of the update during a regularly scheduled or non-scheduled visit to the workshop. Once in the workshop, the process is the same for recall and non-recall updating.

2.2.1. Recall update process

There are legal requirements in most countries that prescribe how the owner of a vehicle must be informed of a fault that is safety related. Each country has its own specific definition of a safety defect, but they are all similar. The definition provided by the UK Vehicle Safety Branch of the Driver and Vehicle Standards Agency is the following:

A safety defect is a failure due to design and/or construction, common to a number of vehicles, which is likely to affect safe operation and pose a significant risk to the driver, occupants or others. Such defects involve sudden and catastrophic failure with little or no warning to enable the driver to take preventative action, and cannot normally be identified by routine maintenance or obvious changes to the vehicle's normal handling or performance. (Vehicle safety defects and recalls: Code of Practice)

In the United States, the US Code for Motor Vehicle Safety (Title 49, Chapter 301) defines motor vehicle safety as:

…the performance of a motor vehicle or motor vehicle equipment in a way that protects the public against unreasonable risk of accidents occurring because of the design, construction, or performance of a motor vehicle, and against unreasonable risk of death or injury in an accident, and includes non-operational safety of a motor vehicle.

A defect includes any defect in performance, construction, a component, or material of a motor vehicle or motor vehicle equipment. Generally, a safety defect is defined as a problem that exists in a motor vehicle or item of motor vehicle equipment that:

- *poses a risk to motor vehicle safety; and,*
- *may exist in a group of vehicles of the same design or manufacture, or items of equipment of the same type and manufacture*

Examples of defects covered by official recalls include:

- Brakes not working
- Unexpected braking
- Unexpected airbag operation
- Fuel leak
- Fire risk
- Sun roof may shatter
- Seatbelt stalk may detach
- Seatbelt malfunction
- Tow bar may detach
- Brake lamps may not illuminate
- Airbag may not function
- Incorrect warning lights may display
- Clutch pedal may detach
- Throttle pedal may detach
- Hand brake self-release
- Wiring harness chafing
- Steering may fail
- Possible wheel hub and brake calliper detachment
- Seat may catch fire
- Door may open during driving
- Driver's seat may recline unexpectedly

The US Department of Transportation National Highway Traffic Safety Administration (US DOT NHTSA) is responsible for issuing vehicle safety standards and to require vehicle manufacturers to recall vehicles that have safety-related defects or do not meet Federal safety standards. NHTSA is responsible for monitoring the manufacturer's corrective action to ensure that the recall campaign has been successfully completed. The Recall Management Division (RMD) maintains the administrative records for all safety recalls, and monitors these recalls to ensure that the scope is appropriate, and that the recall completion rate and remedy are adequate. NHTSA's monitoring of recall performance may lead to the opening of a recall investigation if the facts appear to indicate a problem with the recall adequacy or execution. A recall investigation can result in expanding the scope of previously announced recalls, or in the adjustment of existing recall remedies.

A recall may occur under the following circumstances:

- At the initiative of the manufacturer who discovers a safety issue;
- As the result of a NHTSA investigation; or,
- Following an order by NHTSA via the courts to recall.

If a safety defect is discovered, the vehicle manufacturer must do the following:

1. Notify NHTSA of the defect, including a description of what happens if it is not attended to and what action is required to rectify it.
2. Notify the vehicle owners by registered mail (No e-mail, but standard post; however, a law is being proposed to allow for an e-mail notice in addition to a standard post registered letter.)
3. Notify the dealers and distributors.
4. The defect must be corrected at no charge to the owner if the vehicle is no older than ten years calculated from the date the defect or noncompliance is determined. The age of the vehicle is calculated from the date of sale to the first purchaser.

The manufacturer must make a serious attempt to contact the present owner of the affected vehicles by using both its own records of registered vehicles and matching current state vehicle registration records to identify the current owner. NHTSA provides a web site where recalls are listed so that owners of vehicles who, including those who have not been contacted, can determine if their vehicle is part of the recall.

According to a report issued by Carfax and reported on 10 February by Reuters[7], "One in every 5.4 vehicles on the U.S. roads is in need of repair of a safety issue serious enough to be involved in a federal government recall. There are more than 47 million vehicles in the United States with open recalls, the report states.[8] This is an increase of 27% from one year ago. NHTSA said that in 2015 there were close to 900 recalls affecting a record 51 million vehicles. The highest rates of unfixed vehicles are, in order, Texas, Mississippi, Alaska, Utah and West Virginia.

In Europe, there is a General Product Safety Directive (GPSD) that includes a section on Motor Vehicles (Motor Vehicles Directive-MVD). These apply to type approval for the sale of new vehicles. There is no provision in the MVD for the recall of vehicles under the jurisdiction of an EU body. It is the individual countries that have the jurisdictional responsibility to see to it that vehicle safety defects are corrected, in a similar way to how it is done in the US. The United Kingdom, for example, has an official recall scheme that is overseen by the Vehicle Safety Branch of the Driver and Vehicle Standards Agency (DVSA) working in cooperation with the vehicle manufacturers and the Driver and Vehicle Licensing Agency. There is an official Code of Practice that defines the scope of what is covered and describes the processes to be followed when a potential safety defect is identified in vehicles supplied to UK

[7] www.reuters.com/article/autos-safety-recalls-idUSL2N15P2F3

[8] There are 258.5 million vehicles in operation on U.S. roads as of October, 2015, according to Carfax parent, IHS Inc.

drivers.

In the UK regulations it is stated that if a vehicle owner who has received a safety recall notice ignores it and does not take the vehicle in for repair, he or she is committing an offence of using a defective vehicle. Ignoring a recall may also affect an insurance claim that the driver may make.

The following process is general for safety recalls:

1. Either the government informs the OEM that a recall is required, or the OEM informs the government that a recall will be undertaken.

2. The appropriate ECU supplier is requested to provide a new release. The OEM tests the new software for quality assurance.

3. The supplier ships the software release to the OEM software update server.

4. The OEM identifies all vehicles that are affected by the recall.

5. A list of all affected vehicles is sent to the OEM CRM server. The OEM CRM connects a vehicle to the dealer who sold the vehicle—or to a dealer that has been listed by the customer as being the preferred dealer.

6. The OEM CRM notifies the dealers that a recall is required and provides a list of the vehicles. NB: The OEM vehicle and customer database may not have the names and contact information for either the first or subsequent owners of the vehicles. Matching the vehicles to the owners is the responsibility of the National Sales Companies in each country.

7. The OEM Software Update Server sends the recall update software to all dealers, and the dealers prepare their reprogramming tools for updating the software.

8. The OEM National Sales Company sends a notice via registered mail and e-mail to all affected customers. It also places an update notice on its web site.

9. The vehicle owner drops off the vehicle at the dealer shop and registers at the front desk.

10. The vehicle is brought into a service bay, a technician connects a serial communication tool to the in-vehicle bus to access the targeted ECU, and the update process of the targeted ECU is started. The technician checks the targeted ECU for the new software version to make sure proper re-flashing occurred.

11. Customer data is updated in the OEM Vehicle and Customer Database.

12. The OEM reports the status of the update to the government.

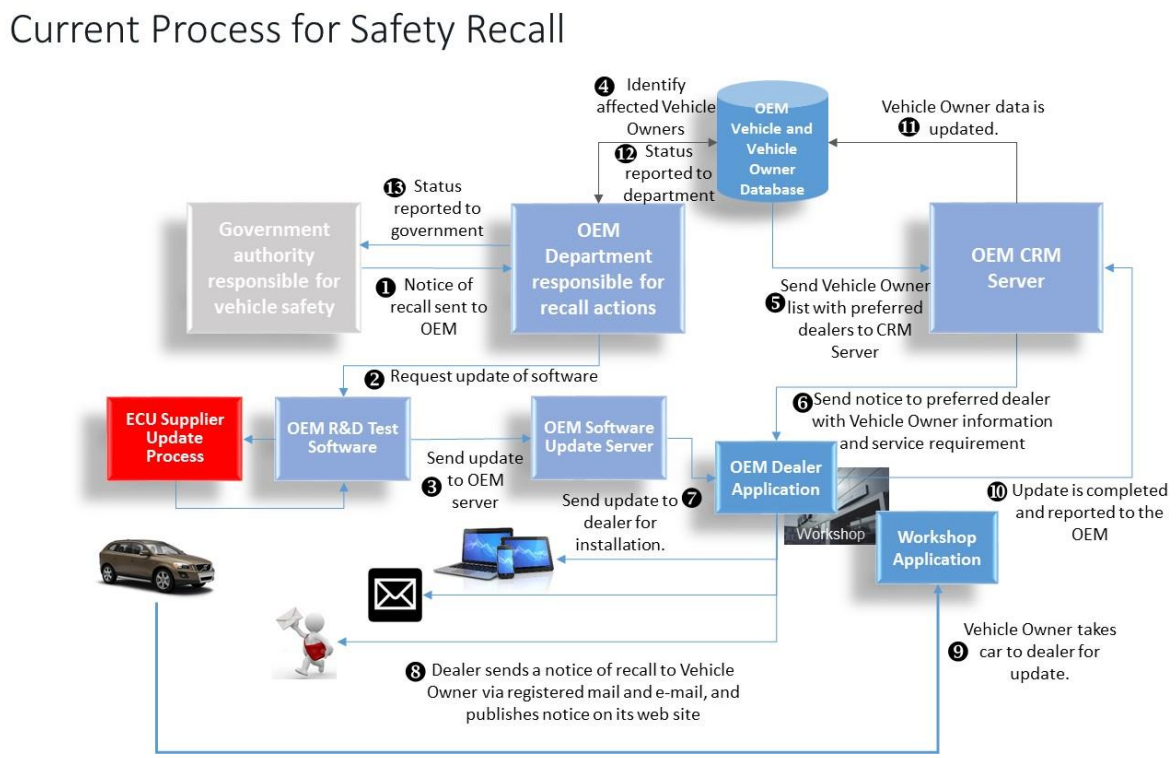


Figure 2: Current process for safety recall

2.2.2. Non-recall operation updates

There are certain types of problems that affect the performance or operation of a vehicle, but which do not pose a safety risk to the driver, the occupants of the vehicle or to pedestrians. These include:

- Air conditioners and radios that do not operate properly.
- Ordinary wear of equipment that has to be inspected, maintained and replaced periodically. Such equipment includes shock absorbers, batteries, brake pads and shoes, and exhaust systems.
- Non-structural or body panel rust.
- Quality of paint or cosmetic blemishes.
- Excessive oil consumption

There are no regulations requiring that these problems are rectified by the OEM, other than what is covered by a new vehicle warranty.

There is, however, a class of non-safety related issues that are covered by regulations in some countries: polluting emissions control. In the US, the Environmental Protection Agency's Office of Transportation and Air Quality is responsible for an air pollution compliance program for all mobile vehicles, engines and equipment, including cars and trucks. All new cars sold in the United States must have an EPA-issued "certificate of conformity" demonstrating that the vehicle meets applicable federal emission standards to control air pollution. The EPA is an agency of the US federal government that was created to protect human health and the environment,

and operates under laws passed by the US Congress, in particular, the Clear Air Act (Effective December 17, 1963 with amendments). The section of the CAA affecting motor vehicles is Title II-Emission Standards for Moving Sources; Part A – Motor Vehicle Emission and Fuel Standards.

Although the Clean Air Act is a federal law covering all fifty states and territories, the states are responsible for carrying out the act. For example, in the case of the VW emissions issue, it was the State of California Air Resources Board that led the initial investigation of the diesel vehicles. It was the EPA that issued on September 18, 2015 a Notice of Violation (NOV) of the Clear Air Act to VW AG, Audi AG and VW Group of America, Inc., alleging that four-cylinder VW and Audi diesel cars sold in the US from model years 2009 to 2015 include software that circumvents EPA emissions standards.

This distinction between federal and state responsibilities is important for what must be done with the software in the vehicles. VW is likely to be fined by the EPA for violating the Clean Air Act, but it is the state regulations that determine whether a vehicle must be fixed. In California, a vehicle must meet the state's emissions standards in order to obtain a registration, which is valid for one year. This is not the case in most other states. This means that a vehicle owner in a state without strict emissions regulations could continue driving a vehicle that is in violation of the US Clean Air Act.

In Europe, EU emission standards define the acceptable limits for exhaust emissions of new vehicles sold in EU member states. These standards are defined in a series of European Union Regulations and Directives staging the progressive introduction of increasingly stringent standards. Regulations are directly applicable in all Member States and therefore have to be adopted into country law exactly as agreed between the European Parliament and the Council. This means that all Member States adopt regulations in the same way (e.g. European eCall is a Regulation). Much of European law takes the form of Directives, which set out general rules and objectives, but leave Member States the choice as to how to attain them.

Non-recall updates are initiated when one or more of the following situations arise:

- A problem is experienced by a driver who takes the vehicle to a dealer. The fault is identified as one that can be fixed with a firmware update. The firmware update is either already downloaded to the workshop application, or it is scheduled for release;
- A problem is identified by the OEM, but it is not a problem that would be experienced by the driver. An update is requested from the ECU supplier, and it is downloaded to the workstation application. The fix is made when a customer takes his or her vehicle in for regular service; or,
- A problem is identified by the OEM when the vehicle sends an OBDII diagnostic trouble code (DTC) to the OEM's remote diagnostic system. The customer is contacted by a dealer and informed that a fix can be made if the vehicle is brought to a dealer.

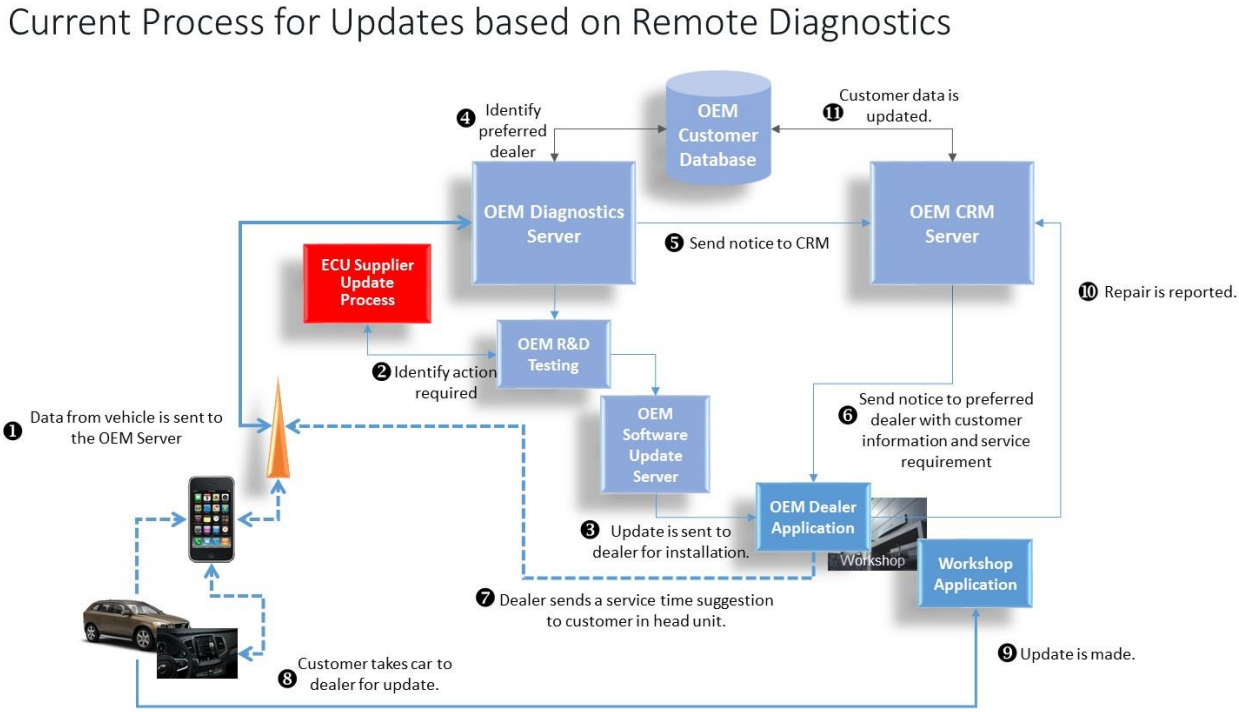


Figure 3: Problem detected when vehicle sends an OBDII diagnostic trouble code

2.2.3. Improvements in performance

Performance improvements include everything that is not related to safety, security or environmental hazards. Since 2012, Mercedes-Benz has been updating the infotainment apps that run on some of its vehicle's head units by letting the *mbrace2* embedded telematics system communicate directly with the smart phone running the apps. This allows the customer to decide which apps it would like to run in the vehicle, rather than having to accept the app supplier chosen by the OEM. Improving driving comfort can also extend how the vehicle handles in different situations. Tesla has shown that even features of vehicles which have been considered fixed until the advent of re-programmable ECUs are now variable. These include rate of acceleration and maximum speed.

Map data content is another area of performance improvement. Navigation map data stored on board the vehicle becomes quickly out-of-date. Even a new vehicle that has had the map data loaded at the time the navigation system was produced, or even downloaded at the end-of-line in the factory, will not have the latest map data by the time a customer takes ownership. When a navigation system cannot provide a needed route as a result of outdated data, it is the OEM's reputation that is tarnished. OEMs have attempted to convince vehicle owners with built-in navigation systems to pay for regular updates with limited success. Some OEMs have included map updates as part of regular service visits, but these may not be more than once per year. Over-the-air updates of navigation map data is an excellent solution for this application since it can take place on a regular basis with no impact on the performance of the

system since the new map data can be cached until it is completely downloaded and then it can be transferred to the primary map data storage device.

BMW is one of several companies currently offering its customers OTA map updates. It is a standard feature for BMW Connected Drive customers. At non-defined but regular intervals, the Connected Drive back-end communicates with the vehicle's on-board unit and initiates a download of incremental map data updates. This ensures that the amount of data needing to be transferred is minimal. The OBU's internal SIM is used for the connectivity. The navigation system is unaffected by the data transfer process. When the downloading is completed, the incremental changes are applied to the map database.

Figure 4: BMW navigation screen showing OTA map update in progress with 97% complete

Tesla has designed its cars from the outset to allow powertrain updates to be delivered over-the-air since most of the company's vehicles allow ECUs to be accessed via the vehicle's central telematics system. Some examples of updates it can make are:

- Improvements to acceleration times
- Remove or reduce restrictions to allow for increases in top speeds
- Location-based air suspension that remembers potholes

The Tesla *Autopilot*, which was announced in July 2015, allows supported cars to steer themselves on motorways, change lanes when their user indicates and even find a spot and parallel park by themselves. Tesla began delivering *Autopilot* to Tesla Model S cars in the United States in September. The over-the-air firmware update to Model S Software Version 7.0 takes advantage of extra detection features that had been included in Tesla vehicles produced since October 2014, including a forward radar, a forward-looking camera, 12 long-range ultrasonic sensors positioned to sense 16 feet around the vehicle in every direction at all speeds, and a high-precision digitally-controlled electric assist braking system. Tesla told owners that the new features were designed to increase "the driver's confidence behind the wheel" and "to help the vehicle avoid hazards and reduce the driver's workload". At a press conference, Tesla CEO Elon Musk told journalists: "We're being especially cautious at this early stage, so we're advising drivers to keep their hands on the wheel just in case." He emphasized that Tesla would not be taking responsibility for any accidents that drivers of its cars get into while using self-driving features.

2.2.4. Security risk corrective action

Researchers have shown that existing wireless connections can allow them to hack into cars and take control of vehicle locks and brakes. Two researchers (see sidebar) were able to successfully break through whatever security shields Fiat Chrysler Automobiles and Sprint set up around its UConnect on-board

systems and wireless network to take control over the most mission critical functions of a Jeep Cherokee. Starting with the climate controls, the radio and the windshield wipers, the attackers moved to the transmission and the brakes. Eventually, the vehicle was brought to a standstill on a major artery in St. Louis, Missouri in the US. The driver of the vehicle, Andy Greenberg, a journalist with *Wired Magazine*, was a willing victim, but his description of his experience in Wired indicated that he was truly frightened while he sat helpless in the vehicle while it was being controlled remotely from ten miles away.

The entire process appears to have been extremely well planned and executed over a two-year period, culminating in having the author of the article that would describe the experience serving as, in his own words, the 'crash dummy'. Miller and Velasek first had to learn to speak 'CAN', the vehicle bus standard intended to link microcontrollers and devices in vehicles to communicate with each other without a host computer. They had to find the most likely candidate for their experiment, which they did, according to Greenberg, by applying for and obtaining "mechanic's accounts on the websites of every major automaker and downloaded dozens of vehicles' manuals and wiring diagrams." They used this information to determine how the on-board systems connected to the Internet, and then which vehicles were the most vulnerable. Jeep Cherokee was selected as the most vulnerable.

They identified one vulnerable access point that lets anyone who knows the vehicle's IP address gain access to a chip in the vehicle's head unit where the chip's firmware is rewritten and new code can be deposited. The new firmware can send commands through CAN to any mission critical component, like the brakes, engine, transmission or sensors. Before the test drive, Miller and Valasek provided Fiat Chrysler Automobiles with enough information to allow the company to issue a recall on July 16th for 1.4 million vehicles to close the security hole in their vehicles.

Miller has said that remote updates will add a new target for hackers, but he notes that so far, no malicious hackers have taken over cars, and he says remote updating systems can be made secure—"It's possible to screw it up. But it's certainly possible to do it right," he says. Even if the change is slow, Miller says, remote software updates for cars are inevitable. As the amount of software in a vehicle—and the potential for bugs—increases, remote updates "are going to have to happen," he says. With the current approach of bringing cars into dealerships, "It can be months before software gets updated. It might never get updated," he says. "That leaves a lot of cars in a vulnerable state."

2.3.Conditions

A vehicle has several different phases in the manufacturing and customer delivery process that affect both its physical location and its availability to be accessed via telecommunications channels. These phases vary from one OEM to another as a result of many different business factors that are OEM-specific. It is possible that these phases could be standardized if there were sufficient financial rewards for doing so, but it would be more efficient if an OTA process could account for the different possibilities.

A vehicle also has a life cycle following delivery to the first customer that is

extremely varied. In the US, the Environmental Protection Agency assumes that a typical vehicle is driven 15,000 miles (24,000 kilometres) per year, and the typical vehicle reaches its end of life at around 200,000 miles (320,000 kilometres). This means that the average vehicle has a life of approximately thirteen years.

OTA updates are only possible if the vehicle's communication device is active, able to receive signals throughout the entire updating process, has sufficient bandwidth to be able to transfer the necessary data files during the update cycle and is able to remain in operation long enough without completely draining the primary battery. Vehicle manufacturers shut down as many of the battery-draining functions as possible when the engine is turned off. Some functions, generally including communications devices, remain on for a period of time in order to access them in case of need, but are eventually turned off if the engine is not started after a period of non-usage.

Having a vehicle at the dealer's workshop is the condition that can guarantee that all of the conditions are unconditionally met. Placing the responsibility of meeting the requirements on the driver may be possible once a vehicle has been purchased, but there are quite a number of conditions prior to a driver taking possession and after a vehicle has been sold where there is no driver. Adding to this complexity are the different states that the vehicle's communications module can be in, which will either allow or not allow wireless access to the vehicle for performing OTA updates.

2.3.1. Location of vehicle

Every vehicle that is manufactured follows a fixed set of steps through the production and final delivery process. These steps are defined by the OEM and what occurs during each step is different for each OEM. The steps below are general for all OEMs up to the point of delivery to the customer. At that point, the processes diverge for the different types of customers: private; fleet lease; rental.

2.3.1.1 End-of-line at factory

Wireless communications units may or may not be active, but the (wired communications) to and from the vehicle are active in order to test that all systems are working and to make last-minute updates to ECU(s).

2.3.1.2 In transport from factory to market

A vehicle can be on a transport truck, a train or a ship. It can also be in transport under its own power, which is often the case with trucks and buses, and in this case it must be taken out of transport mode. When being transported, vehicles are normally in a mode that totally prevents them from being driven or from using battery power, so accessing wireless communications units cannot be guaranteed. In other cases, a vehicle may be driven, but not over a very low speed (e.g. 30 kph). Some vehicle OEMs (e.g. JLR) transmit positions from their vehicles while in transit to allow them to be tracked. This is both for security and to provide customers with better information about delivery.

2.3.1.3 Port of entry

When vehicles reach their final market it is an opportunity to make changes that are market-specific. For example, market-specific SIM-cards can be inserted in SIM-card holders and activated. Vehicles that will eventually be shipped to all dealers in the market can be updated in a single location and then each vehicle can be tested to verify that the update has been competed properly. The same updates that can be performed in a dealer's workshop can be performed in the workshop at the port of entry.

2.3.1.4 In transport from port of entry to dealer

The main difference between this transport is that it is assumed that the vehicle is in the same country where the SIM-card (or equivalent) in the embedded communications unit, or in the external SIM-card slot, is active. If the vehicle was taken out of transport mode at the port of entry, it is normally put back into transport mode again.

2.3.1.5 At dealer prior to pre-delivery inspection

In some markets, such as the US, Canada, Russia and China, the large majority of cars are delivered to dealers and are sold to customers from the dealers' lots. Customers try to find the best combination of price and specification and then select a preferred dealer for post-sale service after the sale is completed. A vehicle can sit on a lot for a few days or several months before it is sold. In other markets, particularly Western Europe, customers visit a dealer and together with a dealer prepare a specification for the vehicle they wish to purchase. The vehicle is ordered and delivered to the dealer who has ordered it. The time between when it arrives at the dealer from the port of entry until when it is delivered to the customer is usually a matter of days. Prior to the pre-delivery inspection (PDI), the vehicle is still in transport mode.

2.3.1.6 At dealer post pre-delivery inspection

A vehicle is taken out of transport mode in order to deliver it to a customer or to use it for demonstration purposes. When it is has been taken out of transport mode it can be driven normally, but not all functions are guaranteed to be active. The embedded communications unit may be active, but it may not be provisioned with the phone call and data messaging routing logic.

2.3.1.7 At dealer for demonstration

A vehicle used for demonstration purposes is normally totally active with all functions accessible, including communications functions. A demonstration vehicle has the dealer as its owner, so any functions that are customer-specific must be reset once the eventual owner takes possession of the vehicle.

2.3.1.8 Vehicle at customer's residence

Following the sale of a vehicle, the owner of the vehicle is added to the record of that vehicle. There is normally a single, authorized driver of the vehicle who is the one notified if there is an official recall, who is contacted in case the vehicle is stolen or who is sent a fine if the vehicle been recorded by a speed

camera or red light detector.

A vehicle at the customer's residence is the most difficult to categorize according to status of engine and availability for communication and power. A residence could be an apartment in a city with the vehicle parked on a public street or in an underground garage. It could be a cabin in the forest with no coverage whatsoever. No process can be defined that would cover all conditions. A process executed at the customer's residence would have to define for the customer the conditions that would need to be met in order to guarantee completion of the update.

2.3.1.9 Vehicle delivered to fleet leasing company

The vehicle will be assigned to a driver by the leasing company, and this driver's name may or may not be known to the dealer who has sold the vehicle or registered in a system that delivers services (e.g. emergency, roadside assistance, stolen vehicle tracking) to the vehicle.

2.3.1.10 Vehicle delivered to vehicle rental/sharing company

The vehicle is normally not assigned to a driver in the OEM's records but is registered with the vehicle rental/vehicle sharing company.

2.3.1.11 In parking garage or parking lot

Neither communications access, electrical power nor customer presence can be guaranteed when a vehicle is in a public parking garage or parking lot.

2.3.1.12 Parked along road

The condition is similar to at the customer's residence with the added difficulties that it may not be possible to control the time the vehicle may remain in the same parking location, there may not be an electric cable in case it is necessary to keep the battery charged for an extended period of time and there may not be a Wi-Fi connection.

2.3.1.13 Operating on a road

The vehicle is in its most accessible mode from the position of cellular connectivity when the engine is running. All systems in the vehicle are active and accessible for communications and the driver is present to receive and respond to messaging. With the engine running, there is reliable electrical power to all ECUs. There are two principal problems with using this time for performing updates:

- The main task to be performed while driving is driving with no distractions. Responding to requests to accept or delay updates is a distraction and should not be performed while the vehicle is moving.

- Continuous Wi-Fi connectivity is not available.

If the driver is presented with a request to perform updates at the start or end of a driving cycle it means that that there will be an unplanned delay at

beginning the drive or when the destination has been reached. Updating during the driving cycle can be compared with starting a session with a PC or mobile device. With PC and mobile phone updates, the user can set the update parameters for different levels of updates and the method for downloading and installing the updates.

2.3.1.14 Other locations

2.3.1.14.1 On ferry

Neither communications access, electrical power nor customer presence can be guaranteed when a vehicle is on a ferry.

2.3.1.14.2 Off road

Neither communications access nor electrical power can be guaranteed when a vehicle is off road.

2.3.1.14.3 In storage (main battery disconnected)

The vehicle is completely inaccessible.

2.3.2. Status of connectivity

There are currently two methods to connect a vehicle to the communications network:

- Cellular – embedded modem with SIM-card/ chip or equivalent; external SIM-card connected to the embedded modem; or tethered phone via cable or Bluetooth providing both the modem and SIM.
- Wi-Fi – the vehicle has a wireless network adaptor which connects either to a stationary network access point or, via tethering (cable or Bluetooth) to a wireless communications device that has a data plan and acts as a modem.

A third method, broadband satellite, is under development.

Each OEM has its own, specific requirements for when an embedded modem is active and able to both transmit and receive data messages. Mobile network operators prefer to have the modems active only when they reach the market where the vehicles will be sold. This is not always possible because an OEM may build vehicles in a few factories in different countries and ship them to countries all around the world. The OEM may wish to perform end-of-line testing of the communications unit, or may wish to be able to track the vehicle from the end of the line all the way to the selling dealer, as JLR does. The communications hardware manufacturer may wish to test the unit as well, and its factory may be in a completely different part of the world than the OEMs' factories.

For these reasons, some OEMs request that the SIM-cards/chips are active when they are delivered to the hardware manufacturer of the embedded unit, and methods have been developed by MNOs and their suppliers to accommodate the OEMs and deliver active SIM-cards/chips in the case of GSM-based modules, and active phone modules in the case of CDMA-based

modules.

2.3.2.1 Cellular

There are various states of cellular connectivity. These states are defined by the OEM in consultation with its telematics control unit and mobile network suppliers. They are established in order for the TCU to provide the needed functionality at each particular location and point in the life cycle of the vehicle. In order to use the cellular communications capability of a vehicle for any part of the OTA process, it is essential to know in which state the cellular connectivity module is set.

2.3.2.1.1 SIM inactive

A SIM is inactive when it is not possible for the modem to obtain the International Mobile Subscriber Identity (IMSI) from the SIM-card/chip, and it is therefore not possible to relay the IMSI to the network in order to make a Request for Access. The embedded modem will therefore not be usable to access the wireless network.

2.3.2.1.2 TCU inactive

A TCU is inactive if it has not been connected to the vehicle network so that it can respond to commands from on-board ECUs or to external communications. This is a state that some OEMs set their TCUs during transport or until the vehicle is delivered to a customer. Even if the SIM is active, it is not possible to communicate to or from the vehicle.

2.3.2.1.3 TCU unprovisioned

Provisioning is the process of delivering to the TCU the phone numbers, data access node numbers and routing logic in order for the TCU to perform the tasks of communicating with service providers. An unprovisioned TCU will be able to communicate with 112/911 emergency services, but will not be able to perform other functions. Provisioning is performed at different times by each OEM. Some provision at the factory; others provision when the vehicle is taken out of transport mode; others provision only when the vehicle is delivered to a customer.

A provisioned TCU can be unprovisioned under certain circumstances:

- Vehicle has been sold to a dealer and there is no current owner of the vehicle. The dealer can unprovision
- Customer does not renew a subscription that is needed for using the TCU and the TSP unprovisions the TCU

2.3.2.1.4 Partially provisioned

Vehicles used for demonstration purposes may be partially provisioned with only emergency routing logic, but not with the ability to process special types of messages, such as software downloading or firmware updating.

2.3.2.1.5 Customer provisioned

A TCU with a customer who is either the authorized driver or the owner of the vehicle acting on behalf of authorized driver is normally fully provisioned. All

services are available to and from the vehicle, and the logic for routing all service requests are resident in the vehicle, either in the TCU or in an ECU that is accessible to the TCU.

2.3.2.1.6 SIM active; TCU active; Provisioned; TCU in sleep mode

In order to avoid draining the primary battery, certain systems are turned off when the engine is not running. Some OEMs have designed their TCUs to remain fully on for a period of time and then to alternate being on or off during another period of time so that certain types of services can be executed. One such service is remote engine start when a vehicle has been in an airport parking garage. The service is turning on the air conditioning or heater so that the vehicle is comfortable when the driver arrives. If the TCU is in sleep mode and does not 'wake up', it is not possible for remote commands to reach it and be executed.

2.3.2.2 Tethered modem

Tethering relates to using a wired (e.g. USB cable, USB key, OBD Dongle) or wireless connections (typically Bluetooth today, but also Wi-Fi) to allow the phone's IP data connection to be shared with the vehicle and should not be confused with other applications of Bluetooth in the vehicle, such as hands-free voice calling.[9] The advantages of using a tethered solution for connectivity services are:

- Requires less costly hardware in-vehicle;
- Is more likely to benefit from up-to-date external modems, given the renewal cycle of mobile devices is faster than that for vehicles;
- Provides direct allocation of service connectivity costs to the end user.

There are challenges with using a tethered solution for any type of connectivity service, including the following:

- No guarantee that the driver will employ the solution consistently enough to maintain service continuity (especially for those services, such as remote diagnostics, which should always be active in the background, but have no immediate "benefit" to the consumer);
- The difficulty in physically securing tethered solutions for safety and security applications (such as eCall, where the phone could be damaged or thrown from the vehicle; or stolen vehicle tracking where the module must be inaccessible from thieves) etc.
- The necessity to have remote connection to the vehicle by the user (i.e. remote control of vehicle environment requires an embedded solution).

2.3.2.3 Wi-Fi

Mobile Wi-Fi hotspots in cars for sharing a single Internet connection are starting to be offered by a number of OEMs, both in Europe and in the US. The difference between an embedded telematics device and a Wi-Fi hotspot is that the embedded device has all it needs to communicate with the wireless

[9] Connecting Cars: Bring your own device – Tethering Challenges; GSMA Connected Living Programme: mAutomotive (February 2013)

network, both for cellular connections (phone, SMS, data transfer) and for Internet connections. When a vehicle OEM states that it has a Wi-Fi hotspot, it can mean different things. In the case of Volvo, GM and Mercedes-Benz, it means that there is a Wi-Fi router that allows multiple devices (smartphones, tablets, laptops) to connect to it, and there is an adapter built into the vehicle, just like there is a Wi-Fi adapter built into most modern laptops and smartphones, that will use an available Internet-connected communications device brought into the vehicle. With Volvo, that device is either a smartphone, or, if Volvo On Call is installed, the device will be the modem in the Volvo On Call system connected to an external SIM-card. OnStar offers Wi-Fi connectivity using the embedded SIM provided by AT&T.

Wi-Fi enabled can also mean that the vehicle is able to be connected to a fixed Wi-Fi hotspot that is outside of the vehicle, such as in a workshop or in the owner's garage. This is similar to connecting a laptop or wireless device to a hotspot in a café or at an airport to avoid high data costs that would be incurred if one used a personal wireless modem or a smartphone data subscription. It is this latter functionality that if of greatest utility for delivering FOTA and SOTA since the cost of using a Wi-Fi hotspot is significantly lower than using a data subscription on a mobile wireless device for delivering large data files. Also, the data rates and connection reliability are both higher.

2.3.3. Authorized driver presence

Any process for informing the owner of a vehicle that an update of any kind can or should be performed must consider the fact that the authorized owner of a vehicle may not be driving the vehicle when a notice is received in the vehicle. This could be due to the following:

- The authorized owner has allowed someone else to drive the vehicle
    - Family member or friend
    - Private vehicle sharing drivers
    - Valet parking driver
    - Car repair driver
    - Leased vehicle driver
- A unauthorized driver is in the vehicle
    - Thief in the process of stealing the vehicle
- The registered owner of the vehicle at the time the notice is sent is different from the registered owner of the vehicle in the data available to the OTAMG.
    - The vehicle has been sold, or its registration transferred to another party, but the record of the registered owner has not been updated.
- Car rental driver

  In the case of rental cars, this will always be the condition. In the case of leased or company cars, the driver may be authorized to receive and act upon update messages. It will depend on the type of agreement the driver has with the leasing company or the employer.

It cannot be assumed that a message sent to a vehicle is received by the person who is authorized to process the message and take the action that is necessary to execute a software update, whether it is a safety or security update or a performance enhancing one.

As an example of how OTA update authorizations are being performed today, computer and smart phone updates are usually classified under the following three levels:

- Important updates – Include those updates that will correct known problems, strengthen the security of the system against unauthorized access and deliver the most up-to-date content. If these updates are not performed, there is a risk that the software will malfunction or that security will be breached.

- Recommended updates – Include those updates that will improve functionality and increase usability. If these updates are not performed, the software will continue to function as it does currently.

- Product updates – Include those updates that relate to software versions in which new functionality is added and system performance is enhanced. The life of the device on which the software is running is extended.

The authorized owner of the device chooses which method to use for downloading and installing the updates, include the following:

- Automatically download and install – This requires pre-authorization by the authorized owner, and this must be confirmed for each of the three non-recall classes and three different levels of updates. Automatically downloading and installing the updates places the responsibility of identifying the location and connectivity of the vehicle on the OTAMG.

- Automatically download updates but let me choose whether to install - This also requires pre-authorization by the authorized owner, and this must be confirmed for each of the three non-recall classes and three different levels of updates. Automatically downloading the updates places the responsibility of identifying the location and connectivity of the vehicle on the OTAMG.

- Inform me of updates and let me choose whether to download and install – This does not require pre-authorization, but requires a method to be informed of the updates, request that they be downloaded or reject them and a method to accept that they are installed or not installed.

Convenience for the owner is the most important consideration when seeking authorization for OTA software updates. The major differences between performing OTA updates on a computer or smart phone versus in a vehicle that the computer or smart phone owner can initiate the OTA and do something else while the downloading is taking place. When the driver enters a vehicle, it is with the intention of driving from the parking location to a destination as quickly as possible. Even responding to queries related to accepting downloads which may be possible to perform during driving is an annoying

hindrance.

There is a similarity with some updates on smart phones that require a Wi-Fi connection, versus using the wireless data connectivity of the subscriber identity module. This is that the update cannot be performed unless the user secures a Wi-Fi connection, and then keeps that Wi-Fi connection active until the update is completed. Apple requires a Wi-Fi connection for its iOS updates, which are a few hundred megabytes large and can take over an hour to complete. It is advisable that the phone is on its charger when such an update is made.

There must be a secure method for confirming that a person receiving and acting on an update message is authorized to accept or reject the update. Each OEM has its own method for securing the identity of an authorized driver or registered owner in those cases when it is necessary to do so, including gaining access to a mobile application that indicates the location of the vehicle, starts the climate controls or unlocks the doors. It should continue to be possible for the OEMs to use their own methods for identity security, rather than forcing a new method specifically related to OTA updates.

2.3.4. Process for re-delivery

It is not uncommon when we update software or drivers on our PCs or smart phone that the process fails, that data is lost or parameters in programs are changed to the point that it makes the applications more difficult to use. This is annoying and sometimes costly to repair, but it is rarely if ever life-threatening. Errors made during the updating of an ECU can have serious negative consequences. Therefore, there needs to be agreed methods to test whether any form of update has been successfully made, whether there are unexpected effects on the performance of other ECUs than the one that has been updated and to revert to the state the vehicle was in prior to the update in case any problem has occurred.

Once the vehicle has reverted to its pre-update state, there should be a process for identifying why the update was not successful, fixing the problem and then re-issuing the update.

2.4. National Standards Regulation and Type Approval Regulation Compliance

2.4.1. U.S. vehicle safety regulations

The most significant change in U.S. vehicle safety regulation came with the National Traffic and Motor Vehicle Safety Act of 1966. Senator Abraham Ribicoff, one of the advocates of the new legislation, said during floor debate: *"This problem is so vast that the Federal Government must have a role. It is obvious the 50 states cannot individually set standards for the automobiles that come into those 50 States from a mass production industry."*

As passed unanimously by both houses of Congress and signed by President Johnson, the legislation had two parts:

- The Highway Safety Act of 1966 mandated that each state put in place a highway safety program in accordance with federal standards that would include improving driver performance, accident records systems and traffic control; and
- The National Traffic and Motor Vehicle Safety Act of 1966 directed the Secretary of Commerce (later changed to the Secretary of Transportation when that agency was established in 1967) to issue safety standards for all motor vehicles beginning in January 1967. A National Traffic Safety Agency was established to carry out the provisions; it was renamed the National Highway Traffic Safety Administration (NHTSA) in 1970.

2.4.1.1 The U.S. Approval Process

Since it was established, NHTSA has issued dozens of safety standards, and it maintains an extensive database on vehicle crashes. However, the agency neither approves motor vehicles or parts as complying with its standards nor collects information from manufacturers as to compliance. The law puts the onus for enforcement of federal standards on automakers themselves. It provides that *"A manufacturer or distributor of a motor vehicle or motor vehicle equipment shall certify to the distributor or dealer at delivery that the vehicle or equipment complies with applicable motor vehicle safety standards prescribed by NHTSA."*

Certification of a vehicle must be shown by a label or tag permanently fixed to the vehicle. The law also makes manufacturers responsible for testing of vehicles and liable for recalls and penalties if they are later found not to meet NHTSA's standards. After a new model is in the market, NHTSA buys vehicles from dealers and tests them at its own facilities to determine whether they comply with current standards. If NHTSA determines there is noncompliance, it can encourage the manufacturer to recall the model to correct the problem, or it can order a recall.

2.4.1.2 U.S. emissions standards

The Environmental Protection Agency (EPA) and the California Air Resources Board (ARB) are the two main authorities responsible for emissions legislation for mobile and stationary sources. These authorities both define emissions legislation in addition to assessing a manufacturer's compliance with the requirements.

In order to meet the emission standards set by the federal government, the federal government requires that every manufacturer offer a limited warranty emissions control on the vehicles they build. The Federal Emission Warranty covers any repairs needed to correct defects in materials or workmanship which would cause the vehicle not to meet the Environmental Protection Agency (EPA) standards. Most components that fall under the federal emissions warranty are covered for 2 years or 24,000 miles, whichever comes first. The catalytic converter, emissions control unit (ECU), and the on board emissions diagnostic device (OBD) are covered for 8 years or 80,000 miles whichever comes first.

There are two parts to the emission warranty: Performance Warranty and a

Design and Defect Warranty. The Performance Warranty covers components that are listed under the federal emissions warranty if the vehicle fails an emissions test. If the vehicle fails a state mandatory emissions test, then the performance warranty will cover the cost of repairing or replacement of any component covered as long as it is within the time and mileage limits. According to federal law, the Design and Defect Warranty covers "an emission control or emission related part, or a specified major emission control component, that fails because of a defect in materials or workmanship, must be repaired or replaced by the vehicle manufacturer free of charge as long as the vehicle has not exceeded the warranty time or mileage limitations for the failed part."

In order to receive warranty repairs, the vehicle must be taken to an authorized service centre. If the repair shop is not authorized to perform repairs then the federal emissions warranty will not cover the cost. Since the federal emission warranty applies for only 2 years or 24,000 miles for most components, most manufacturers' factory warranties cover the components after the emission warranty expires. Beyond the expiration of the factory warranty, an extended auto warranty may cover the components depending upon the level of coverage.

2.4.2. EU vehicle safety regulations

In contrast to the U.S. system of self-certification, the comparable EU vehicle system is based on government regulatory approval in advance of manufacturing. Until the 1950s, European vehicle safety regulations developed separately in each country. Interest in harmonizing vehicle regulation emerged as part of the process of European economic integration. The European vehicle regulatory regime now includes both EU directives, which must be implemented by all member states, and standards promulgated through a United Nations organization (United Nations Economic Commission for Europe-UNECE), which may be implemented at the discretion of a national government.

2.4.2.1 European Approval Process

The system of type approval based around EC Directives provides for the approval of whole vehicles, vehicle systems, and separate components. Type approval is the confirmation that production samples of a design will meet specified performance standards. The specification of the product is recorded and only that specification is approved. Automotive EC Directives require third party approval - testing, certification and production conformity assessment by an independent body. Each Member State is required to appoint an Approval Authority to issue the approvals and a Technical Service to carry out the testing to the Directives and Regulations. An approval issued by one Authority will be accepted in all twenty-eight Member States.

2.4.2.2 European Community Whole Vehicle Type Approval (ECWVTA)

EC Whole Vehicle Type Approval (ECWVTA) is based around EC Directives and provides for the approval of whole vehicles, in addition to vehicle systems and separate components. This certification is accepted throughout the EU without the need for further testing until a standard is updated or your design

changes.

Low volume/Small Series Manufacturers

Full EC whole vehicle type approval (ECWVTA) won't suit everyone, particularly those manufacturing vehicles in low numbers. In recognition of this fact there are a number of other approval routes available, including:

European Community Small Series Type Approval (EC SSTA)

EC Small Series Type Approval) has been created for low volume vehicle producers only, and like full ECWVTA will allow Europe wide sales but with technical and administrative requirements that are more adapted to smaller businesses.

National Small Series Type Approval (NSSTA)

(National Small Series Type Approval) is a UK national scheme for low volume manufacturers who intend to sell only in the UK. The advantages of NSSTA are relaxed technical requirements for some subjects, a more pragmatic approach to the Conformity of Production (CoP) requirements, and reduction in administrative requirements. Like ECWVTA, once the design is approved, individual vehicles do not need to be tested.

Individual Vehicle Approval (IVA)

Individual Vehicle Approval is a UK national scheme and the most likely route for those manufacturing or importing single vehicles or very small numbers. IVA does not require CoP as it is based on inspection of each vehicle, although most bodybuilders and converters will work with manufacturers to ensure there is no warranty compromise. Under IVA, vehicles have to be inspected by the Vehicle and Operator Services Agency (VOSA) in Great Britain or the Driver and Vehicle Agency (DVA) in Northern Ireland.

2.4.2.3 European emissions standards

The European Commission is responsible for defining the emissions standards that must be met by products sold/operated within countries in the European Union. The assessment of a manufacturer's compliance with the regulations is verified by an independent type approval authority, of which there are over 30 operating throughout Europe.

2.4.3. United Nations Agreement

In 1952, the United Nations (UN) established the Working Party on the Construction of Vehicles—known as Working Party 29 or WP. 29—a subsidiary body of the Inland Transport Committee of the United Nations Economic Commission for Europe (UNECE). The objective of WP.29 is to *"initiate and pursue actions aimed at the worldwide harmonization or development of technical regulations for vehicles."* WP.29 administers a 1958 agreement on vehicle construction and two related agreements which were adopted by some European countries to promote EU-wide integration of vehicle construction, environmental protection and safety.

UNECE regulations deal with harmonized performance requirements on vehicle safety, environmental protection, fuel efficiency, and anti-theft devices. Signatories to the 1958 UN agreement commit to mutual recognition of approvals for vehicle components so that a component approved for use in one signatory country will be automatically recognized in all others. UN regulations do not yet cover the whole vehicle, but still only its parts. WP.29's voting members are limited to government representatives, but automakers, trade associations, and other nongovernmental organizations also participate in its meetings. The United States of America did not sign the 1958 UN agreement because it would require mutual recognition of standards generated outside the United States. After U.S. self-certification began in 1967, the UNECE approach was seen as incompatible with the U.S. process. Because the United States remained outside of the 1958 UN Agreement, many U.S.-made vehicles could not be exported to many countries without modifications. However, the United States of America did sign a 1998 UN global agreement which establishes global technical regulations (GTRs), effectively transforming the UN body into an organization with a global approach now called the World Forum for Harmonization of Vehicle Regulations. It promulgates worldwide harmonized regulations affecting vehicle safety, environmental protection, energy efficiency, and anti-theft performance. Unlike the 1958 UN agreement, there are no administrative requirements for type approval and mutual recognition of approvals. GTRs are established in a UN Global Registry and contracting parties use their own national or regional regulatory process to implement them.

The technical provisions of a new GTR specifying the test method for vehicles, their parts and equipment, as well as the performance requirements, are in general incorporated into the existing UN Regulations or a new UN Regulation annexed to the 1958 UN agreement. Therefore, the 1998 UN global agreement and the 1958 UN agreement are in fact parallel agreements.

2.5. National Standards Initiatives for Security Risk Mitigation

The issue of vehicle cybersecurity has been elevated to the very highest level of focus by the U.S., Japan and the countries of Europe. They have recognized that the benefits of avoiding crashes as a result of deploying electronic safety technologies also pose challenges with respect to cybersecurity.

2.5.1. United States

NHTSA has outlined its approach to vehicle cybersecurity on its website.[10] It states:

> *To ensure a robust cybersecurity environment for these dynamic new technologies, NHTSA modified its organizational structure, developed vital partnerships, adopted a layered research approach, considered legislative additions, and encouraged members of the industry to take independent steps to help improve the cybersecurity posture of vehicles in the United*

[10] http://www.nhtsa.gov/About+NHTSA/Speeches,+Press+Events+&+Testimonies/NHTSA+and+Vehicle+Cybersecurity

States. NHTSA's goal is be ahead of potential vehicle cybersecurity challenges, and seek ways to address or avoid them altogether.

Extracts below are taken from the NHTSA and Vehicle Cybersecurity report.

In 2012, NHTSA modified its research organization to focus on vehicle electronics, including cybersecurity. It established a new division, Electronic Systems Safety Research, to conduct research on the safety, security, and reliability of complex, interconnected, electronic vehicle systems. More recently, NHTSA expanded its research and testing capabilities in vehicle electronics at the Vehicle Research and Test Center in East Liberty, Ohio. Together, these entities execute research programs in three main areas:

1. Electronics reliability (including Functional Safety)
2. Automotive cybersecurity
3. Automated vehicles

They are responsible for evaluating, testing, and monitoring potential automotive cyber vulnerabilities, and for leading the agency's research of highly automated vehicles.

NHTSA also established an internal agency working group, the Electronics Council. This council is responsible for collaborating more broadly on issues related to vehicle electronics, including cybersecurity, across the entire NTHSA organization.

In October 2014, NHTSA published four cybersecurity reports that describe the agency’s initial work to support the goals outlined in its Automotive Cybersecurity Research Program.

• Assessment of the Information Sharing and Analysis Center Model

This report presented findings from an assessment of the ISAC model, and how ISACs are effectively implemented in other sectors. The report also explains how a new sector ISAC could be formed by leveraging existing ISAC models. This report was sent directly to the Association of Global Automakers and Alliance of Automobile Manufacturers to aid with their automotive ISAC activities.

• A Summary of Cybersecurity Best Practices

This report documented results from the analysis and review of best practices and observations across a variety of industries in the field of cybersecurity involving electronic control systems. It provides benchmarks for the agency and the industry.

• Characterization of Potential Security Threats in Modern Automobiles: A Composite Modeling Approach

This report described a composite modeling approach for potential cybersecurity threats in modern vehicles. Threat models, threat descriptions, and examples of various types of conceivable threats to automotive systems

are included, along with a matrix containing a condensed version of the various potential attacks.

• National Institute of Standards and Technology (NIST) Cybersecurity Risk Management Framework Applied to Modern Vehicles

This report reviewed the NIST guidelines and foundational publications from an automotive cybersecurity risk management standpoint. The NIST approach is often used as a baseline to develop a more targeted risk management approach for use in specific industries and sectors.

NHTSA's research program takes a layered approach to cybersecurity for automobiles. It assumes that all entry points into the vehicle, such as Wi-Fi, infotainment, the OBD-II port, and other points of potential access to vehicle electronics, could be potentially vulnerable. This way, NHTSA focuses on solutions to harden the vehicle's electrical architecture against potential attacks and to ensure vehicle systems take appropriate safe steps even when an attack may be successful. A layered approach to vehicle cybersecurity reduces the probability of attack and mitigates the potential ramifications of a successful intrusion.

At the vehicle level this approach includes the following four main areas:

- Protective/preventive measures and techniques: These measures, such as isolation of safety-critical control systems networks or encryption, implement hardware and software solutions that lower the likelihood of a successful hack and diminish the potential impact of a successful hack.

- Real-time intrusion (hacking) detection measures: These measures continually monitor signatures of potential intrusions in the electronic system architecture.

- Real-time response methods: These measures mitigate the potential adverse effects of a successful hack, preserving the driver's ability to control the vehicle.

- Assessment of solutions: This involves methods such as information sharing and analysis of a hack by affected parties, development of a fix, and dissemination of the fix to all relevant stakeholders (such as through an ISAC). This layer ensures that once a potential vulnerability or a hacking technique is identified, information about the issue and potential solutions are quickly shared with other stakeholders.

NHTSA also has examined whether legislative provisions might further improve the cybersecurity posture of vehicles. The U.S. Department of Transportation (USDOT)'s GROW AMERICA legislative proposal includes liability for hackers, clarifying authority for the agency to issue process rules or guidelines for the safe development of new systems, and imminent hazard authority that would enable swift action to protect the public from cybersecurity vulnerabilities and other safety threats. We believe the legislative proposals contained in GROW AMERICA will allow the agency to stay ahead of cybersecurity challenges.

The NHTSA report concludes with the following:

> *No single approach is sufficient because in the cybersecurity realm, those involved must keep moving, adapting, and improving. To that end, NHTSA will continue to explore numerous approaches, including internal research, independent testing, analysis conducted by the agency, and communication. NHTSA cannot do this alone, but neither can vehicle manufacturers or suppliers. Our efforts will need to be collective, collaborative, and complete.*

2.5.2. Japan

Japan Automobile Research Institute (JARI) is a non profit organization supported by more than 200 organizations in auto industry, electric industry and other fields. The mission of JARI is to investigate common issue in automotive industry, such as safety, and do research on the future automobile and automotive environment, such as ITS. JARI also has a mission of exploring and spreading new technologies to member organizations and also to general public. JARI's stated role is to analyse U.S. and European automotive strategies in order to assist Japan's car industry with developing products that have a high competitiveness in terms of performance, quality and cost. JARI studies research and standardization trends in all areas, including cooperative systems.

It is JARI that serves as the secretariat of ISO/TC 204/WG1: Architecture and Terminology. In addition to promoting discussion of Japan's draft standard proposals, JARI also actively participates in the activities of ISO/TC 204/WG16 (Wide Area Communication) and ISO/TC 204/WG17 (Nomadic Devices), among other working groups. The diagram below, provided by JARI, shows the relationships among the various standards bodies and where JARI contributes.

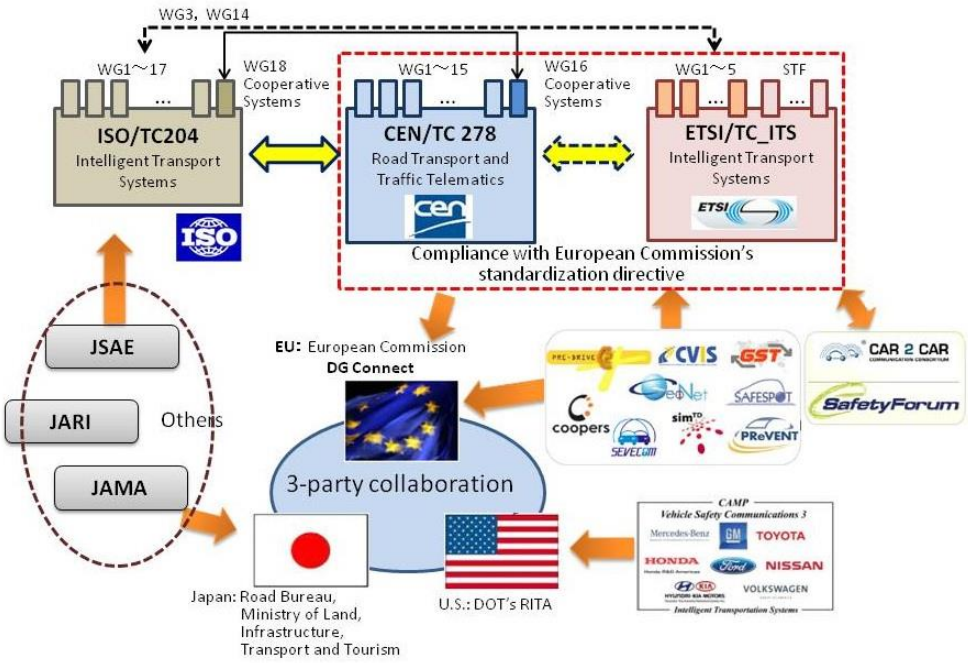


Figure 5: International Standardization Activities Concerning ITS

The issue of personal data protection and assurance of vehicle systems security have been major concerns for JARI since 2002, when it initiated studies on the topics after detailed analysis of probe vehicle information protection.

JARI has prepared a vision of tomorrow's motorized society based on the results of studies on ITS R&D/standardization activities and the results of surveys concerning trends in the market environment surrounding the automotive industry, ITS and related policy measures. JARI is examining an action plan for resolving various technical issues and social system issues in order to present proposals for ushering in the motorized society desired in the future and encouraging efforts to make it a reality. Security is a key part of the roadmap JARI has prepared, both at the higher and lower levels of communication.

JARI's autonomous driving and vehicle platooning activities have an important cybersecurity component. It states:

> *As driver assistance systems become more sophisticated with the aim of facilitating autonomous driving, the increased system complexity will require that the reliability of the advanced technologies used be raised to even higher levels. JARI is engaged in various activities to enhance reliability further, including development of the ISO 26262 standard for the functional safety of automotive electronic systems and promoting the effective application of tools like fault tree analysis (FTA) and failure mode and effects analysis (FMEA), among others.*

2.5.3. Europe

The European Union Agency for Network and Information Security (ENISA) is responsible for researching computing threats to countries in the EU, including hacking vehicles. ENISA was set up to enhance the capability of the European Union, the EU Member States and the business community to prevent, address and respond to network and information security problems. In order to achieve this goal, ENISA is a Centre of Expertise in Network and Information Security and is stimulating the cooperation between the public and private sectors.

The Agency's regulation based tasks are focused on:

Advising and assisting the Commission and the Member States on information security and in their dialogue with industry to address security-related problems in hardware and software products.

- Collecting and analysing data on security incidents in Europe and emerging risks.
- Promoting risk assessment and risk management methods to enhance our capability to deal with information security threats.
- Awareness-raising and co-operation between different actors in the

information security field, notably by developing public / private partnerships with industry in this field.

A new ENISA focus on vehicle security following the presentations made on security gaps in Chrysler, GM and Tesla cars means that its researchers are going to be investigating how to formulate the policies that the EU can use to standardize approaches to vehicle cybersecurity.

The ENISA Work Programme 2016 [11] includes a section devoted to cybersecurity for smart cars.

WPK1.1. Improving the expertise related to critical information infrastructures

Desired impact:

- By 2017, national authorities in at least five MS use ENISA's recommendations on smart cars and intelligent road systems.
- By 2017, national authorities in at least five MS use ENISA's recommendations on smart health devices, services and infrastructures.
- By 2017, national authorities in at least five MS use ENISA's recommendations on smart airports.

Description of tasks

In this WPK ENISA aims to develop good practices on emerging smart critical infrastructures and services using the concept of the internet of things (IoT) to deliver new, innovative business models and services. An infrastructure can be defined as smart when investments in human and social capital and traditional (transport) and modern (ICT) communication infrastructure support sustainable economic development and a high quality of life, with wise management of natural resources, through participatory action and engagement.

The reports will provide smart critical information infrastructure and service providers and developers with good security and resilience practices when designing, developing and deploying such services in order to minimise the exposure of such network and services to all relevant cyberthreat categories. This builds on previous work of ENISA in the area of smart cities (WP 2015), smart grids (WP 2012-2015) and intelligent transportation systems (WP 2015).

The main areas of work of this WPK are as follows.

Smart cars and intelligent road systems (not including public transportation means). ENISA, in cooperation with national competent authorities, will identify smart car and vehicle manufacturers and operators and will take stock of cybersecurity risks and challenges introduced by the use of IoT. The Agency will then develop good practices for private and public stakeholders (e.g.

[11] https://www.enisa.europa.eu/publications/programmes-reports/enisa-work-programme-2016

national competent authorities).

Smart health services and infrastructures. ENISA will identify e-health critical service providers (e.g. hospitals, e-health cloud providers, insurance companies, smart laboratories) and will take stock of major cybersecurity risks and challenges introduced by the use of IoT. The Agency will then develop good practices for both private as well as public stakeholders (e.g. national competent authorities).

Smart airports including supply chain integrity. ENISA will identify major airports that develop and operate smart services and take stock of the security challenges arising from the usage of these services. The Agency will then develop good practices for airports and relevant public authorities that address these challenges.

These emerging areas are selected based on their criticality for citizens and the economy. The Agency expects these particular sectors and services to benefit the most from the wide adoption of IoT and machine to machine (M2M) technologies. The early adoption of these good practices will boost trust and confidence of potential users of such infrastructures and pave the way for the wide deployment of them. In this way ENISA will help EU industry to become more competitive and innovative.

For each area ENISA will identify all relevant public and private stakeholders, engage them in working groups and jointly take stock of and analyse the current situation in terms of cybersecurity and resilience giving emphasis on communication security. The Agency will also identify EU and national-funded projects in the area of IoT and M2M communication, liaise with them, analyse their findings and deliverables, and further engage them in corresponding expert groups. Special emphasis will be given to the resilience and robustness of such smart critical information.

3. Operational Requirements

There are six phases of an FOTA or SOTA update once a decision has been taken by the vehicle OEM to perform an update:

1. Prepare the update.
2. Obtain regulatory approvals for the update, if required.
3. Obtain the necessary permissions to perform the update from the authorized driver or registered owner.
4. Manage the update end-to-end.
5. Confirm receipt and proper functioning of the update.
6. Perform administrative tasks.

Each of these phases must be considered in relation to the **Conditions** of the vehicle (location and status of connectivity), the presence of the **Authorized Driver** and the process for an attempt to **Re-deliver** the update if the primary process fails.

OR-OTA: 0-001.1

Each OEM providing OTA updates should have a group that is designated to manage the end-to-end firmware and software over-the-air update delivery process (OTA Management Group-OTAMG).

3.1. Update preparation

3.1.1. Classify the update

OR-OTA: 1-001.1

The process starts with identifying the nature of the update required. All other processes will depend on whether the update is classified as one of the following:

OR-OTA: 1-001.1.1 – Recall update

OR-OTA: 1-001.1.2 – Non-recall operation updates

OR-OTA: 1-001.1.3 – Performance improvement updates

OR-OTA: 1-001.1.4 – Security risk correction action updates

3.1.2. Determine conditions

When and how the update may be delivered will depend on the **Location** of the vehicle and the **Status of Connectivity**.

OR-OTA: 1-002.1

All locations of the vehicle prior to delivery to the customer should be known by the OEM. The status of connectivity to the vehicle is under the control of the

OEM during this period.

For each of the four classes of updates, identify the processes to be used for each of the following pre-delivery locations:

OR-OTA: 1-002.1.1 - End-of-line at factory

OR-OTA: 1-002.1.2. - In transport from factory to market

OR-OTA: 1-002.1.3. - Port of entry

OR-OTA: 1-002.1.4. - In transport from port of entry to dealer

OR-OTA: 1-002.1.5. - At dealer prior to pre-.delivery inspection

OR-OTA: 1-002.1.6. - At dealer post pre-delivery inspection

OR-OTA: 1-002.1.7. - At dealer for demonstration

Following customer delivery, the location and connectivity status are much more variable and are under the control of the authorized driver or vehicle owner. For each of the four classes, identify the processes to be used for the following locations according to the status of connectivity:

OR-OTA: 1-002.2.1 - At customer's residence

OR-OTA: 1-002.2.2 - At fleet leasing company

OR-OTA: 1-002.2.3 - At vehicle rental/sharing company

OR-OTA: 1-002.2.4 - In a parking garage or parking lot

OR-OTA: 1-002.2.5 - Parked along road

OR-OTA: 1-002.2.6 - Operating on a road

OR-OTA: 1-002.2.7 - On a ferry

OR-OTA: 1-002.2.8 - Off road

OR-OTA: 1-002.2.9 - In storage with main battery disconnected

3.1.3. Define process for re-delivery

OR-OTA: 1-003.1

When updates are not completed successfully and have to be re-delivered, there need to be technical and business processes for performing the re-delivery. These process should be defined for each of the classes of updates in combination with each of the conditions.

OR-OTA: 1-003.1.1 – Re-delivery process for recall

OR-OTA: 1-003.1.2 – Re-delivery process for non-recall operations

OR-OTA: 1-003.1.3 – Re-delivery process for performance improvement

OR-OTA: 1-003.1.4 – Re-delivery process for security risk correction

3.2. Regulatory approvals

A change to ECU software or firmware may affect the performance of that ECU, or the vehicle component and vehicle systems that are controlled by the ECU, in such a way that the type approval or regulatory standards compliance are affected. If this is the case, the update must be designed so that the performance of the ECU and affected components and systems will pass the type approval process or comply with relevant regulatory standards.

3.2.1. Determine which regulatory standards are affected

OR-OTA: 2-001.1

Determine if a change made to firmware or software on an ECU will change the performance of a component, vehicle system or the vehicle with respect to a regulatory standard for safety.

OR-OTA: 2-001.2

Determine if a change made to firmware or software on an ECU will change the performance of a component, vehicle system or the vehicle with respect to a regulatory standard for emissions.

3.2.2. Determine if Type Approval/Standards Compliance is required

OR-OTA: 2-002.1.1

Determine if the update will require a new component type approval.

OR-OTA: 2-002.1.2

Determine if the update will require whole vehicle type approval.

OR-OTA: 2-002.1.3.

Determine if the update will require new verification of compliance to a safety regulations standard.

OR-OTA: 2-002.1.4.

Determine if the update will require new verification of compliance to an emissions regulation standard.

3.2.3. Obtain Type Approval/Comply with Standards if required

OR-OTA: 2-003.1.1

Obtain new component type approval, if required.

OR-OTA: 2-003.1.2

Obtain whole vehicle type approval, if required.

OR-OTA: 2-003.1.3.

Obtain new verification of compliance to a safety regulations standard, if required.

OR-OTA: 2-003.1.4.

Obtain new verification of compliance to an emissions regulation standard, if required.

3.3. Permissions to perform update

Prior to the delivery of a firmware or software over-the-air update, the authorized driver or registered owner of the vehicle must be notified, and permission must be obtained for performing the update. The authorized driver or registered owner is not necessarily the person driving the vehicle at any particular time, so once the contact details of the authorized driver or registered owner are known, a method of informing the authorized driver or registered owner must be executed.

3.3.1. Identify authorized driver or registered owner

OR-OTA: 3-001.1

The name and contact details of the authorized driver or registered owner, either a physical or legal person, who has the authority to accept or reject an update, must be available to the OTAMG.

3.3.2. Define method of informing authorized driver or registered owner

OR-OTA: 3-002.1

Informing authorized drivers or registered owners of updates will be performed either by a central OTAMG, by the National Sales Companies or by the OEM Dealers. This decision will be made by the respective OEMs. Decide who will inform the authorized driver or registered owner for each of the classes.

OR-OTA: 3-002.1.1

Decide who will inform the authorized driver or registered owner in case of a recall.

OR-OTA: 3-002.1.2

Decide who will inform the authorized driver or registered owner in case of a non-recall operation.

OR-OTA: 3-002.1.3.

Decide who will inform the authorized driver or registered owner in case of a performance improvement.

OR-OTA: 3-002.1.4.

Decide who will inform the authorized driver or registered owner in case of a security risk correction.

OR-OTA: 3-002.2

The method of informing the driver will depend on both the class of update and the location of the vehicle. Alternative methods outside the vehicle, which could be used in combination, are:

OR-OTA: 3-002.2.1 - Registered letter for recall updates is mandatory. A method based only on sending a message to the vehicle is not acceptable

OR-OTA: 3-002.2.2 - Unregistered letter

OR-OTA: 3-002.2.3 - E-mail

OR-OTA: 3-002.2.4 - SMS

OR-OTA: 3-002.2.5 - Social media (e.g. Twitter, Instagram, WeChat)

OR-OTA: 3-002.2.6 - OEM website

OR-OTA: 3-002.3

If the method of informing the drivers includes a data message sent to the vehicle, this message should be prepared and authorized by the OTAMG and delivered to the vehicle in a secure manner with full traceability.

OR-OTA: 3-002.4

Alternative methods inside the vehicle, which could be used in combination with methods from outside the vehicle, are:

OR-OTA: 3-002.4.1 - Text on display screen at engine start

OR-OTA: 3-002.4.2 - Text on display screen at engine stop

OR-OTA: 3-002.5

In the case that the name of the authorized driver or registered owner are incorrect, an effort shall be made to identify the correct authorized driver or registered owner and update the records with this information.

3.3.3. Define method for obtaining authorization to perform update

OR-OTA: 3-003.1

The authorized driver or registered owner must consent to any update performed on the vehicle. This authorization will take a different form for each of the four classes of updates (Recall, etc.), and there will be different types of

authorization for various levels of updates within the non-recall classes.

OR-OTA: 3-003.2

There must be a secure method for confirming that a person receiving and acting on an update message is authorized to accept or reject the update. This method must accommodate the methods used by each OEM for securing the identity of an authorized driver or registered owner of its vehicles.

OR-OTA: 3-003.2.1

Obtain authorization for the update from the authorized driver or registered owner in case of a recall. For Recall updates, the country-specific officially-accepted procedure must be followed.

OR-OTA: 3-003.2.2

Obtain authorization for the update from the authorized driver or registered owner in case of a non-recall operation.

OR-OTA: 3-003.2.3.

Obtain authorization for the update from the authorized driver or registered owner in case of a performance improvement.

OR-OTA: 3-003.2.4.

Obtain authorization for the update from the authorized driver or registered owner in case of a security risk correction.

3.4. End-to-end update management

3.4.1. OTAMG Processes

The OTAMG will follow the process devised by each OEM to identify the source of the problem that an OTA update will fix or the improvement that the OEM or its ECU supplier has recommended for delivery to customers.

OR-OTA: 4-001.1

There needs to be a FOTA/SOTA Update Delivery Platform that is capable of delivering vehicle-specific updates on a global basis, or regional nodes that manage vehicles in each of the OEM's markets. This platform shall:

OR-OTA: 4-001.1.1

Manage the various versions of the update packages

OR-OTA: 4-001.1.2

Handle the actual network delivery of the packages to the correct vehicle model and its specific ECU.

OR-OTA: 4-001.1.3

Deliver the appropriate confirmations to all parties as required.

OR-OTA: 4-001.2

In the short term, the centralized software package repository used for FOTA/SOTA will not replace the standard distribution of software updates to systems used by OEM workshops and independent workshops authorized by OEMs. It will therefore be essential that the version management on the FOTA/SOTA Update Delivery Platform is identical to the software management used for distributing software to the workshops.

3.4.2. Generate update

OR-OTA: 4-002.1

The FOTA or SOTA will be developed by the supplier of the ECU. Requirements for the update will be specified by the OEM's R&D department, and the resulting update will be tested by the OEM prior to release for each variant of the ECU in the markets where the updates will be made.

OR-OTA: 4-002.1.1 – The OEM will document confirmation that purpose of update is satisfied

OR-OTA: 4-002.1.2 – The OEM will document conformity of the update to regulations

OR-OTA: 4-002.1.3 – The OEM will document confirmation that there are no unintended effects on vehicle systems

3.4.3. Package and deliver the update for delivery

OR-OTA: 4-003.1

There may be a difference between the update that is eventually delivered over-the-air and an update that would be downloaded to a workshop system and delivered in the current non-OTA manner. The OTA update may be a delta package, replacing only the code that has changed, while the workshop update may replace all of the code on the ECU with new code.

OR-OTA: 4-003.2

How the OTA update is performed should be at the discretion of the OEM.

3.4.4. Apply the update

OR-OTA: 4-004.1

The downloaded update package is used to perform the actual update by re-flashing the original firmware and/or software. Because there is usually a limited amount of memory resources on the ECU, the update code and FOTA software should occupy as small an amount of space as possible on the ECU.

OR-OTA: 4-004.1.1 - Before applying the update, the FOTA update software should validate that the correct update package for the vehicle to which it has been delivered has been received.

OR-OTA: 4-004.1.2 - Once confirmed, the re-flashing should proceed.

OR-OTA: 4-004.1.3 - There should be a confirmation that the update process has been successfully completed.

OR-OTA: 4-004.2

If the update process is not successful, a notification shall be sent to the OTAMG system.

3.5. Confirm receipt and proper functioning

Once the update has process has been completed, the authorized driver or registered owner of the vehicle must be informed of the result, and given instructions on how to proceed.

3.5.1. Receive confirmation of successful delivery

OR-OTA: 5-001.1

A message shall be sent to the vehicle as well as to at least one other destination (e.g., SMS, e-mail) specified by the authorized driver or registered owner to be displayed to the authorized driver or registered owner of the vehicle that the OTA update has been successfully completed.

OR-OTA: 5-001.2

The message shall inform the authorized driver or registered owner of the exact steps to be taken to complete the process, including, at a minimum, sending a return confirmation that the successful completion is acknowledged.

OR-OTA: 5-001.3

The process for delivering the return confirmation shall be included in the OTA method implemented by the OEM.

3.5.2. Receive confirmation of unsuccessful delivery

OR-OTA: 5-002.1

A message shall be sent to the vehicle as well as to at least one other destination (e.g., SMS, e-mail) specified by the authorized driver or registered owner to be displayed to the authorized driver or registered owner of the vehicle that the OTA update has <u>not</u> been successfully completed.

OR-OTA: 5-002.2

The message shall inform the authorized driver or registered owner of the exact steps to be taken to re-do the process, including, at a minimum, sending a return confirmation that the <u>unsuccessful</u> completion is acknowledged.

OR-OTA: 5-002.3

The process for delivering the return confirmation shall be included in the OTA method implemented by the OEM.

3.5.3. Re-issue update if unsuccessful

OR-OTA: 5-003.1

If the OTA update is unsuccessful, determine the possible reason for the failure.

OR-OTA: 5-003.2

If the failure is not the result of any processes up to the point that it is sent to the vehicle, repeat the process starting with OR-OTA: 4-003.1.

3.6. Perform administrative tasks

3.6.1. Communications with authorities

3.6.1.1 Process recall notice from authorities

OR-OTA: 6-001.1.1 – Receive recall notice from authorities and initiate process of recall.

3.6.1.2 Report status to authorities

OR-OTA: 6-001.1.1 – At prescribed intervals, report status of all vehicles that are subject to recall.

3.6.2. Update internal OEM records

OR-OTA: 6-002.1

Update all internal records with the status of all vehicles that have been subject to an OTA update of any kind.

3.6.3. Distribute payments for the updates to all involved parties

OR-OTA: 6-003.1

Disbursements of payments to all parties involved in the provision and delivery of OTA updates must be part of the end-to-end process.

OR-OTA: 6-003.2

Payment routines must be considered from the outset. They will be OEM-specific and potentially even market-specific.

4. Functional Requirements

These functional requirements address the four use cases for which FOTA/SOTA will be applied:

1. Recall updates
2. Non-recall operation updates
3. Improvements in performance
4. Security risk corrective action

4.1. Recall

Once a safety defect that requires a recall has been made by the authorities, a manufacturer has three options for correcting the defect. These are:

- Repair the defect;
- Replace the vehicle with an identical or similar vehicle; or,
- Refund the full purchase price of the vehicle, minus a reasonable allowance for depreciation.

The defect can affect one or more ECUs, or can involve a physical part that must be repaired or replaced.

Affected vehicles include all those manufactured in the country where the recall is being made (referred to as 'domestic vehicles') as well all those manufactured outside the country and brought into the country via a port or ports of entry (referred to as 'imported vehicles').

A recall is announced at a particular point in time, either when the governmental agency in charge of recall management makes a final decision that a defect must be remedied by a recall, or when a manufacturer makes the determination to conduct a recall. On this date, vehicles will be in different locations with varying levels of connectivity available, as described in Section 2.3.

- *The requirements listed in Section 4 are for repairing the defect.*
- *The requirements listed in Section 4 are for performing a recall remedy that involves the updating of one or more ECUs, not for repairing or replacing physical parts.*
- *The requirements listed in Section 4 are for repairing defects in both domestic and imported vehicles.*
- *The requirements listed in Section 4 are for addressing the repair of defects at any location considering the availability of connectivity to the vehicle manufacturers' systems that will be used to perform the update to the affected ECU(s).*

4.1.1. End-of-line at factory

FR-OTA: 1-001.1

Following an official recall that can be rectified by the updating of one or more ECUs, all affected vehicles shall have the affected ECU(s) updated prior to leaving the production line when the modifications can be tested and confirmed as completed.

FR-OTA: 1-001.2

Updating of the ECU(s) shall be made using the manufacturer's IT systems.

FR-OTA: 1-001.3

Vehicles that contain ECUs which are affected by a recall, but which have not been updated in the factory, shall be clearly identified to the OTAMG so that they may be updated at the next available time.

4.1.2. In transport from factory to market (or to dealer for domestic vehicles)

FR-OTA: 1-002.1

When a recall is officially announced, all vehicles that are in transport from the factory to the market where the recall is to be made shall be clearly identified in the manufacturer's vehicle database by the OTAMG so that these vehicles can be updated at the next available time.

FR-OTA: 1-002.2

Since connectivity to a cellular or Wi-Fi network cannot be guaranteed while a vehicle is being transported by road, rail, ship or under its own power in transport mode, no attempt shall be made to update a vehicle's ECUs during the time a vehicle is in transport.

4.1.3. At port of entry (for imported vehicles)

FR-OTA: 1-003.1

After a recall is officially announced, all vehicles that are affected by the recall which arrive to the port of entry in the market where the recall is to be made shall be clearly identified in the manufacturer's vehicle database. It is up to the vehicle manufacturer to decide if the updates to the affected ECU(s) can be made at the port of entry or if they shall wait until a later time.

FR-OTA: 1-002.2

ECU(s) affected by a recall may be updated at the port of entry by the manufacturer's standard methods used in its authorized workshops.

FR-OTA: 1-002.2.1 - One method is to physically connect a vehicle to a workshop system, perform the update and confirm that the update has been properly made and no other ECU(s) or vehicle systems have been affected.

FR-OTA: 1-002.2.2 - Alternatively, a vehicle manufacturer may determine that vehicles affected by a recall may be updated at the port of entry using OTA processes.

FR-OTA: 1-002.3

When OTA processes are used to update the affected ECU(s), port of entry personnel shall ensure the following:

FR-OTA: 1-002.3.1 - The vehicle has the necessary connectivity to a cellular wireless or Wi-Fi network during the required time for the update to be completed.

FR-OTA: 1-002.3.2 - The vehicle has the necessary battery life to allow the vehicle to complete the update.

FR-OTA: 1-002.3.3 - A confirmation is obtained that the update to the affected ECU(s) has been successfully completed.

FR-OTA: 1-002.3.4 - A confirmation is obtained that the update has not affected any other ECU(s) or vehicle functions.

FR-OTA: 1-002.4

Vehicles that contain ECU(s) which are affected by a recall and which have not been updated at the port of entry shall be clearly identified so that they may be updated at the next available time.

4.1.4. In transport from port of entry to dealer

FR-OTA: 1-004.1

When a recall is officially announced, all vehicles in a market where the recall is to be made that are in transport from the port of entry to the dealer shall be clearly identified in the manufacturer's vehicle database by the OTAMG so that they can be updated when they arrive to the dealer.

FR-OTA: 1-004.2

Since connectivity to a cellular or Wi-Fi network cannot be guaranteed while a vehicle is being transported, no attempt shall be made to update a vehicle's ECU(s) during the time a vehicle is in transport.

4.1.5. At dealer

4.1.5.1 Prior to per-delivery inspection

FR-OTA: 1-005.1.1 - When a recall is officially announced, all vehicles in a market where the recall is to be made that have not had the defect remedied prior to arrival at a dealer shall be identified and made ready for the required update during the pre-delivery inspection process.

4.1.5.2 During pre-delivery inspection

FR-OTA: 1-005.1.2.1 - When a recall is officially announced, all vehicles in a market where the recall is to be made that have not had the defect remedied prior to the pre-delivery inspection process shall, at the discretion of the dealer, have the affected ECU(s) updated during the pre-delivery inspection process.

FR-OTA: 1-005.1.2.2 - ECU(s) affected by a recall may be updated during the pre-delivery inspection process by the manufacturer's standard methods used in its authorized workshops. One method is to physically connect a vehicle to a workshop system, perform the update and confirm that the update has been properly made and no other ECU(s) or vehicle systems have been affected. Alternatively, a vehicle manufacturer may determine that vehicles affected by a recall may be updated in the workshop using OTA processes.

FR-OTA: 1-005.1.2.3 - When OTA processes are used to update the affected ECU(s), dealer personnel shall ensure the following:

FR-OTA: 1-005.1.2.3.1 - The vehicle has the necessary connectivity to a cellular wireless or Wi-Fi network during the required time for the update to be completed.

FR-OTA: 1-005.1.2.3.2 - The vehicle has the necessary battery life to allow the vehicle to complete the update.

FR-OTA: 1-005.1.2.3.3 - A confirmation is obtained that the update to the affected ECU(s) has been successfully completed.

FR-OTA: 1-005.1.2.3.4 - A confirmation is obtained that the update has not affected any other ECU(s) or vehicle functions.

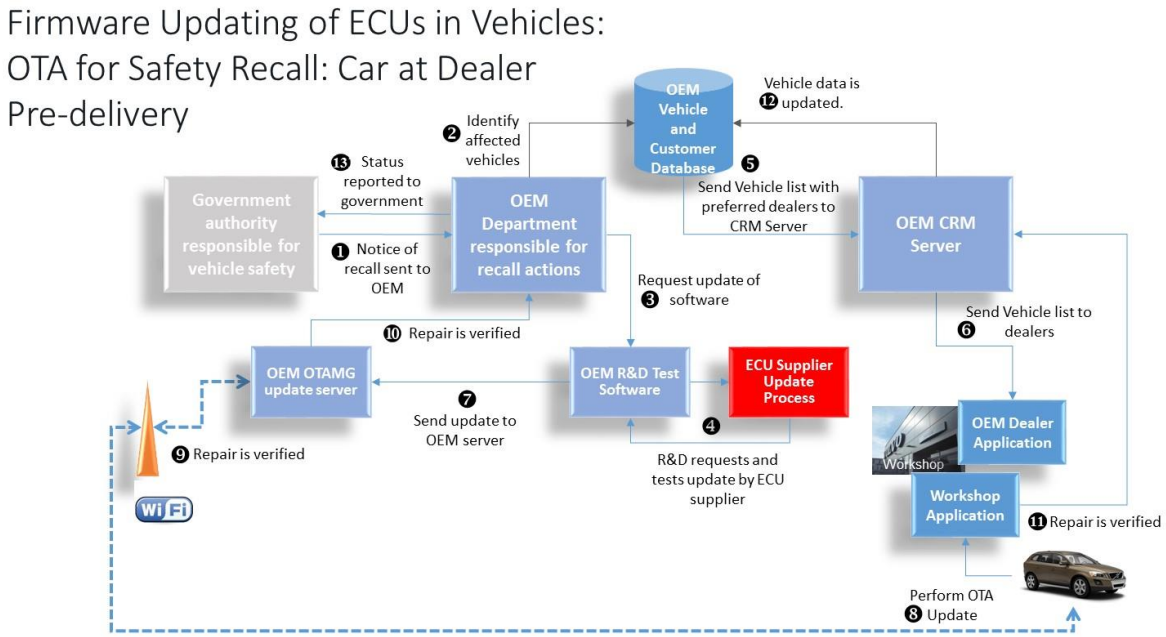


Figure 6: OTA Update Pre-delivery at Dealer

4.1.5.3 Demonstration mode

FR-OTA: 1-005.1.3.1 - When a recall is officially announced, all vehicles in a market where the recall is to be made that have the defect, and are being used for demonstration purposes, shall have the defect remedied immediately or the vehicle shall be taken out of service until the defect is remedied.

FR-OTA: 1-005.1.3.2 - If the defect is remedied using OTA, the conditions listed in FR-OTA: 1-005.1.2.3 shall apply.

4.1.5.4 Post sale prior to delivery

FR-OTA: 1-005.4.1.1 - When a recall is officially announced, all vehicles in a market where the recall is to be made that have the defect, and that have been sold to a customer, but have not yet been delivered to a customer, shall have the defect remedied immediately.

FR-OTA: 1-005.4.1.2 - If the defect is remedied using OTA, the conditions listed in FR-OTA: 1-005.1.2.3 shall apply.

4.1.6. At registered owner's or authorized driver's residence

FR-OTA: 1-006.1

An authorized driver or registered owner of a vehicle must be notified of a recall by the vehicle manufacturer within a 'reasonable time' after the final decision has been taken to initiate a recall.

FR-OTA: 1-006.1.1 – According to current regulations, this notification must be delivered by registered mail.

FR-OTA: 1-006.1.2 - A recall notice shall not be sent to the vehicle for display on the vehicle's head unit as a substitute for or alternative to a registered letter unless this method is explicitly allowed by the applicable regulations in the jurisdiction where the recall has been made.

FR-OTA: 1-006.2

Obtain authorization from the authorized driver or registered owner of the vehicle to perform the recall update.

FR-OTA: 1-006.2.1 – If the vehicle is brought to a dealer, the act of bringing the vehicle to the dealer and registering for the update shall constitute authorization.

FR-OTA: 1-006.2.2 – If the vehicle is not brought to a dealer and the authorized driver or registered owner wishes to have the update performed using OTA, authorization must be provided in a manner that confirms acceptance of the OTA process and securely identifies that the confirmation is being provided by the authorized driver or registered owner.

FR-OTA: 1-006.3

Deliver instructions to the authorized driver or registered owner of the vehicle

on how the update will be performed, what responsibilities he or she has prior to, during and after the update, and what to do in case the update is not successfully completed.

FR-OTA: 1-006.4

When OTA processes are used to update the affected ECU(s), the authorized driver or registered owner shall be instructed to ensure the following:

FR-OTA: 1-006.4.1 - The vehicle has the necessary connectivity to a cellular wireless or Wi-Fi network during the required time for the update to be completed.

FR-OTA: 1-006.4.2 - The vehicle has the necessary battery life to allow the vehicle to complete the update.

FR-OTA: 1-006.4.3 - A confirmation is obtained that the update to the affected ECU(s) has been successfully completed.

FR-OTA: 1-006.4.4 - A confirmation is obtained that the update has not affected any other ECU(s) or vehicle functions.

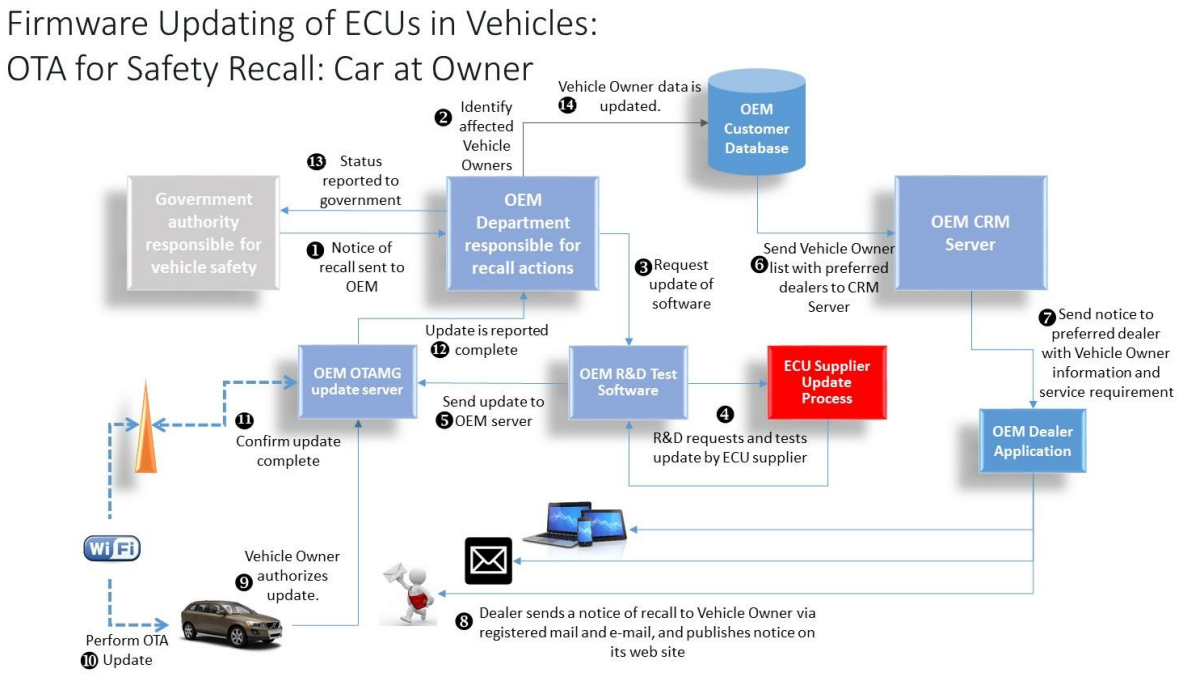


Figure 7: OTA Update Post Delivery at Owner's Residence

4.1.7. During the driving cycle

A driving cycle is the period when a vehicle is being driven by the authorized driver or registered owner. It varies in terms of distance travelled, length of time between ignition off and ignition off, time of day and season of year.

4.1.7.1 Operating on road

FR-OTA: 1-007.1.1 – When a recall is officially announced, all vehicles in a

market where the recall is to be made will be notified of the recall. This notification shall occur according to FR-OTA: 1-006.1.

FR-OTA: 1-007.1.2 – No update of a vehicle's ECU(s) affected by a recall shall be made during a driving cycle while the vehicle is operating on a road with the motor running.

4.1.7.2 Stationary on road

FR-OTA: 1-007.2.1 – No update of a vehicle's ECU(s) affected by a recall shall be made during a driving cycle while the vehicle is operating on a road with the motor running, including when the vehicle is stationery (e.g., stopped at a traffic light).

4.1.7.3 Parked along a road

FR-OTA: 1-007.3.1 – An update of a vehicle's ECU(s) affected by a recall may be made during a driving cycle while the vehicle is stationary and parked along a road if, and only if, the following conditions can be met:

FR-OTA: 1-007.3.1.1 - The vehicle has the necessary connectivity to a cellular wireless or Wi-Fi network during the required time for the update to be completed.

FR-OTA: 1-007.3.1.2 - The vehicle has the necessary battery life to allow the vehicle to complete the update.

FR-OTA: 1-007.3.1.3 - A confirmation is obtained that the update to the affected ECU(s) has been successfully completed.

FR-OTA: 1-007.3.1.4 - A confirmation is obtained that the update has not affected any other ECU(s) or vehicle functions.

FR-OTA: 1-007.3.2. - If the defect is remedied using OTA, the conditions listed in FR-OTA: 1-005.1.2.3 shall apply

4.1.8. Stationary in parking garage or on parking lot

FR-OTA: 1-008.1

An update of a vehicle's ECU(s) affected by a recall may be made during a driving cycle while the vehicle is stationary and parked along a road if, and only if, the following conditions can be met:

FR-OTA: 1-008.1.1 - The vehicle has the necessary connectivity to a cellular wireless or Wi-Fi network during the required time for the update to be completed.

FR-OTA: 1-008.1.2 - The vehicle has the necessary battery life to allow the vehicle to complete the update.

FR-OTA: 1-008.1.3 - A confirmation is obtained that the update to the affected ECU(s) has been successfully completed.

FR-OTA: 1-008.1.4 - A confirmation is obtained that the update has not affected any other ECU(s) or vehicle functions.

FR-OTA: 1-008.2

If the defect is remedied using OTA, the conditions listed in FR-OTA: 1-005.1.2.3 shall apply

4.1.9. Other locations

4.1.9.1 On a ferry

FR-OTA: 1-009.1.1 - Since connectivity to a cellular or Wi-Fi network cannot be guaranteed while a vehicle is on a ferry, no attempt shall be made to update a vehicle's ECU(s) during the time a vehicle is on a ferry.

4.1.9.2 Off road

FR-OTA: 1-009.2.1 - Since connectivity to a cellular or Wi-Fi network cannot be guaranteed while a vehicle is off road, no attempt shall be made to update a vehicle's ECU(s) during the time a vehicle is off road.

4.1.9.3 In storage (main battery disconnected)

FR-OTA: 1-009.3.1 - Since connectivity to a cellular or Wi-Fi network cannot be guaranteed while a vehicle is in storage, and no power is available to the vehicle, no attempt shall be made to update a vehicle's ECU(s) during the time a vehicle is in transport.

4.1.10. Re-delivery

4.1.10.1 Broken communications

FR-OTA: 1-010.1.1 – Failure of a recall update due to broken communications shall be repeated from the initiation of the notification of the update from the OTAMG.

FR-OTA: 1-010.1.2 – The re-delivery will be repeated only once before taking other corrective action, including visiting an authorized workshop where the update may be performed in a closely managed environment.

4.1.10.2 Software failure

FR-OTA: 1-010.2.1 – Failure of a recall update due to software failure shall not be repeated.

FR-OTA: 1-010.2.2 – Following the failure of a recall update to software failure, the authorized driver or registered owner shall be instructed to take the vehicle to an authorized workshop where the update may be performed in a closely managed environment.

4.2. Non-recall Operation Updates

4.2.1. End-of-line at factory

FR-OTA: 2-001.1

Following a decision to perform an operation update that can be rectified by the updating of one or more ECUs, all affected vehicles shall have the affected ECU(s) updated prior to leaving the production line when the modifications can be tested and confirmed as completed.

FR-OTA: 2-001.2

Updating of the ECU(s) shall be made using the manufacturer's IT systems.

FR-OTA: 2-001.3

Vehicles that contain ECU(s) which are affected by an operation update, but which have not been updated in the factory, shall be clearly identified to the OTAMG so that they may be updated at the next available time.

4.2.2. In transport from factory to market (or to dealer for domestic vehicles)

FR-OTA: 2-002.1

When an operation update is officially announced, all vehicles that are in transport from the factory to the market where the operation update is to be made shall be clearly identified in the manufacturer's vehicle database by the OTAMG so that these vehicles can be updated at the next available time.

FR-OTA: 2-002.2

Since connectivity to a cellular or Wi-Fi network cannot be guaranteed while a vehicle is being transported by road, rail, ship or under its own power in transport mode, no attempt shall be made to update a vehicle's ECU(s) during the time a vehicle is in transport.

4.2.3. Port of entry

FR-OTA: 2-003.1

After an operation update is officially announced, all vehicles that are affected by the operation update which arrive to the port of entry in the market where the operation update is to be made shall be clearly identified in the manufacturer's vehicle database. It is up to the vehicle manufacturer to decide if the updates to the affected ECU(s) can be made at the port of entry or if they shall wait until a later time.

FR-OTA: 2-003.2

ECU(s) affected by an operation update may be updated at the port of entry by the manufacturer's standard methods used in its authorized workshops.

FR-OTA: 2-003.2.1 - One method is to physically connect a vehicle to a workshop system, perform the update and confirm that the update has been properly made and no other ECU(s) or vehicle systems have been affected.

FR-OTA: 2-003.2.2 - Alternatively, a vehicle manufacturer may determine that vehicles affected by an operation update may be updated at the port of entry using OTA processes.

FR-OTA: 2-003.3

When OTA processes are used to update the affected ECU(s), port of entry personnel shall ensure the following:

FR-OTA: 2-003.3.1 - The vehicle has the necessary connectivity to a cellular wireless or Wi-Fi network during the required time for the update to be completed.

FR-OTA: 2-003.3.2 - The vehicle has the necessary battery life to allow the vehicle to complete the update.

FR-OTA: 2-003.3.3 - A confirmation is obtained that the update to the affected ECU(s) has been successfully completed.

FR-OTA: 2-003.3.4 - A confirmation is obtained that the update has not affected any other ECU(s) or vehicle functions.

FR-OTA: 2-003.4

Vehicles that contain ECU(s) which are affected by an operation update and which have not been updated at the port of entry shall be clearly identified so that they may be updated at the next available time.

4.2.4. In transport from port of entry to dealer

FR-OTA: 2-004.1

When a operation update is officially announced, all vehicles in a market where the operation update is to be made that are in transport from the port of entry to the dealer shall be clearly identified in the manufacturer's vehicle database by the OTAMG so that they can be updated when they arrive to the dealer.

FR-OTA: 2-004.2

Since connectivity to a cellular or Wi-Fi network cannot be guaranteed while a vehicle is being transported, no attempt shall be made to update a vehicle's ECU(s) during the time a vehicle is in transport.

4.2.5. At dealer

4.2.5.1 Prior to per-delivery inspection

FR-OTA: 2-005.1.1 - When an operation update is officially announced, all vehicles in a market where the operation update is to be made that have not had the defect remedied prior to arrival at a dealer shall be identified and made ready for the required update during the pre-delivery inspection process.

4.2.5.2 Post pre-delivery inspection

FR-OTA: 1-005.1.2.1 - When an operation update is officially announced, all vehicles in a market where the operation update is to be made that have not had the defect remedied prior to the pre-delivery inspection process shall, at the discretion of the dealer, have the affected ECU(s) updated during the pre-delivery inspection process.

FR-OTA: 1-005.1.2.2 - ECU(s) affected by an operation update may be updated during the pre-delivery inspection process by the manufacturer's standard methods used in its authorized workshops. One method is to physically connect a vehicle to a workshop system, perform the update and confirm that the update has been properly made and no other ECU(s) or vehicle systems have been affected. Alternatively, a vehicle manufacturer may determine that vehicles affected by an operation update may be updated in the workshop using OTA processes.

FR-OTA: 1-005.1.2.3 - When OTA processes are used to update the affected ECU(s), dealer personnel shall ensure the following:

FR-OTA: 1-005.1.2.3.1 - The vehicle has the necessary connectivity to a cellular wireless or Wi-Fi network during the required time for the update to be completed.

FR-OTA: 1-005.1.2.3.2 - The vehicle has the necessary battery life to allow the vehicle to complete the update.

FR-OTA: 1-005.1.2.3.3 - A confirmation is obtained that the update to the affected ECU(s) has been successfully completed.

FR-OTA: 1-005.1.2.3.4 - A confirmation is obtained that the update has not affected any other ECU(s) or vehicle functions.

4.2.5.3 Demonstration mode

FR-OTA: 1-005.1.3.1 - When an operation update is officially announced, all vehicles in a market where the operation update is to be made that have the defect, and are being used for demonstration purposes, shall have the defect remedied immediately or the vehicle shall be taken out of service until the defect is remedied.

FR-OTA: 1-005.1.3.2 - If the defect is remedied using OTA, the conditions listed in FR-OTA: 1-005.1.2.3 shall apply.

4.2.5.1 Post sale prior to delivery

FR-OTA: 2-005.4.1.1 - When an operation update is officially announced, all vehicles in a market where the operation update is to be made that have the defect, and that have been sold to a customer, but have not yet been delivered to a customer, shall have the defect remedied immediately.

FR-OTA: 2-005.4.1.2 - If the defect is remedied using OTA, the conditions listed in FR-OTA: 2-005.1.2.3 shall apply.

4.2.6. At registered owner's or authorized driver's residence

FR-OTA: 2-006.1

An authorized driver or registered owner of a vehicle should be notified of an operation update by the vehicle manufacturer within a 'reasonable time' after the final decision has been taken to initiate an operation update.

FR-OTA: 2-006.1.1 – Regulations on how the notification shall be delivered vary by jurisdiction and should be followed accordingly.

FR-OTA: 2-006.1.2 - An operation update notice may be sent to the vehicle for display on the vehicle's head unit as a substitute for or alternative to the recommended notification method unless this method is explicitly disallowed by the applicable regulations in the jurisdiction where the operation update has been made.

FR-OTA: 2-006.2

Obtain authorization from the authorized driver or registered owner of the vehicle to perform the operation update.

FR-OTA: 2-006.2.1 – If the vehicle is brought to a dealer, the act of bringing the vehicle to the dealer and registering for the update shall constitute authorization.

FR-OTA: 2-006.2.2 – If the vehicle is not brought to a dealer and the authorized driver or registered owner wishes to have the update performed using OTA, authorization must be provided in a manner that confirms acceptance of the OTA process and securely identifies that the confirmation is being provided by the authorized driver or registered owner.

FR-OTA: 2-006.3

Deliver instructions to the authorized driver or registered owner of the vehicle on how the update will be performed, what responsibilities he or she has prior to, during and after the update, and what to do in case the update is not successfully completed.

FR-OTA: 2-006.4

When OTA processes are used to update the affected ECU(s), the authorized driver or registered owner shall be instructed to ensure the following:

FR-OTA: 2-006.4.1 - The vehicle has the necessary connectivity to a cellular wireless or Wi-Fi network during the required time for the update to be completed.

FR-OTA: 2-006.4.2 - The vehicle has the necessary battery life to allow the vehicle to complete the update.

FR-OTA: 2-006.4.3 - A confirmation is obtained that the update to the affected ECU(s) has been successfully completed.

FR-OTA: 2-006.4.4 - A confirmation is obtained that the update has not affected any other ECU(s) or vehicle functions.

4.2.7. During the driving cycle

4.2.7.1 Operating on road

FR-OTA: 2-007.1.1 – When an operation update is officially announced, all vehicles in a market where the operation update is to be made will be notified of the operation update. This notification shall occur according to FR-OTA: 2-006.1.

FR-OTA: 2-007.1.2 – No update of a vehicle's ECU(s) affected by an operation update shall be made during a driving cycle while the vehicle is operating on a road with the motor running.

4.2.7.2 Stationary on road

FR-OTA: 2-007.2.1 – No update of a vehicle's ECU(s) affected by an operation update shall be made during a driving cycle while the vehicle is operating on a road with the motor running, including when the vehicle is stationery (e.g., stopped at a traffic light).

4.2.7.3 Parked along a road

FR-OTA: 2-007.3.1 – An update of a vehicle's ECU(s) affected by an operation update may be made during a driving cycle while the vehicle is stationary and parked along a road if, and only if, the following conditions can be met:

FR-OTA: 2-007.3.1.1 - The vehicle has the necessary connectivity to a cellular wireless or Wi-Fi network during the required time for the update to be completed.

FR-OTA: 2-007.3.1.2 - The vehicle has the necessary battery life to allow the vehicle to complete the update.

FR-OTA: 2-007.3.1.3 - A confirmation is obtained that the update to the affected ECU(s) has been successfully completed.

FR-OTA: 2-007.3.1.4 - A confirmation is obtained that the update has not affected any other ECU(s) or vehicle functions.

FR-OTA: 2-007.3.2. - If the defect is remedied using OTA, the conditions listed in FR-OTA: 2-005.1.2.3 shall apply

4.2.8. Stationary in parking garage or on parking lot

FR-OTA: 2-008.1

An update of a vehicle's ECU(s) affected by an operation update may be made during a driving cycle while the vehicle is stationary and parked along a road if, and only if, the following conditions can be met:

FR-OTA: 2-008.1.1 - The vehicle has the necessary connectivity to a cellular wireless or Wi-Fi network during the required time for the update to be completed.

FR-OTA: 2-008.1.2 - The vehicle has the necessary battery life to allow the

vehicle to complete the update.

FR-OTA: 2-008.1.3 - A confirmation is obtained that the update to the affected ECU(s) has been successfully completed.

FR-OTA: 2-008.1.4 - A confirmation is obtained that the update has not affected any other ECU(s) or vehicle functions.

FR-OTA: 2-008.2

If the defect is remedied using OTA, the conditions listed in FR-OTA: 2-005.1.2.3 shall apply

4.2.9. Other locations

4.2.9.1 On a ferry

FR-OTA: 2-009.1.1 - Since connectivity to a cellular or Wi-Fi network cannot be guaranteed while a vehicle is on a ferry, no attempt shall be made to update a vehicle's ECU(s) during the time a vehicle is on a ferry.

4.2.9.2 Off road

FR-OTA: 2-009.2.1 - Since connectivity to a cellular or Wi-Fi network cannot be guaranteed while a vehicle is off road, no attempt shall be made to update a vehicle's ECU(s) during the time a vehicle is off road.

4.2.9.3 In storage (main battery disconnected)

FR-OTA: 2-009.3.1 - Since connectivity to a cellular or Wi-Fi network cannot be guaranteed while a vehicle is in storage, and no power is available to the vehicle, no attempt shall be made to update a vehicle's ECU(s) during the time a vehicle is in transport.

4.2.10. Re-delivery

4.2.10.1 Broken communications

FR-OTA: 2-010.1.1 – Failure of an operations update due to broken communications shall be repeated from the initiation of the notification of the update from the OTAMG.

FR-OTA: 2-010.1.2 – The authorized driver or registered owner shall decide how many times the re-delivery will be repeated before taking other corrective action, including visiting an authorized workshop where the update may be performed in a closely managed environment.

4.2.10.2 Software failure

FR-OTA: 2-010.2.1 – Failure of an operations update due to software failure shall be repeated from the initiation of the notification of the update from the OTAMG.

FR-OTA: 2-010.2.2 – The authorized driver or registered owner shall decide how many times the re-delivery will be repeated before taking other corrective action, including visiting an authorized workshop where the update may be

performed in a closely managed environment.

4.3. Improvements to Performance

4.3.1. End-of-line at factory

FR-OTA: 3-001.1

Following a decision to perform an update of performance that can be completed by the updating of one or more ECUs, all affected vehicles shall have the affected ECU(s) updated prior to leaving the production line when the modifications can be tested and confirmed as completed.

FR-OTA: 3-001.2

Updating of the ECU(s) shall be made using the manufacturer's IT systems.

FR-OTA: 3-001.3

Vehicles that contain ECU(s) which are affected by an update of performance, but which have not been updated in the factory, shall be clearly identified to the OTAMG so that they may be updated at the next available time.

4.3.2. In transport from factory to market (or to dealer for domestic vehicles)

FR-OTA: 3-002.1

When an update of performance is officially announced, all vehicles that are in transport from the factory to the market where the update of performance is to be made shall be clearly identified in the manufacturer's vehicle database by the OTAMG so that these vehicles can be updated at the next available time.

FR-OTA: 3-002.2

Since connectivity to a cellular or Wi-Fi network cannot be guaranteed while a vehicle is being transported by road, rail, ship or under its own power in transport mode, no attempt shall be made to update a vehicle's ECU(s) during the time a vehicle is in transport.

4.3.3. Port of entry

FR-OTA: 3-003.1

After an update of performance is officially announced, all vehicles that are affected by the update of performance which arrive to the port of entry in the market where the update of performance is to be made shall be clearly identified in the manufacturer's vehicle database. It is up to the vehicle manufacturer to decide if the updates to the affected ECU(s) can be made at the port of entry or if they shall wait until a later time.

FR-OTA: 3-003.2

ECU(s) affected by an update of performance may be updated at the port of entry by the manufacturer's standard methods used in its authorized workshops.

FR-OTA: 3-003.2.1 - One method is to physically connect a vehicle to a workshop system, perform the update and confirm that the update has been properly made and no other ECU(s) or vehicle systems have been affected.

FR-OTA: 3-003.2.2 - Alternatively, a vehicle manufacturer may determine that vehicles affected by an update of performance may be updated at the port of entry using OTA processes.

FR-OTA: 3-003.3

When OTA processes are used to update the affected ECU(s), port of entry personnel shall ensure the following:

FR-OTA: 3-003.3.1 - The vehicle has the necessary connectivity to a cellular wireless or Wi-Fi network during the required time for the update to be completed.

FR-OTA: 3-003.3.2 - The vehicle has the necessary battery life to allow the vehicle to complete the update.

FR-OTA: 3-003.3.3 - A confirmation is obtained that the update to the affected ECU(s) has been successfully completed.

FR-OTA: 3-003.3.4 - A confirmation is obtained that the update has not affected any other ECU(s) or vehicle functions.

FR-OTA: 3-003.4

Vehicles that contain ECU(s) which are affected by an update of performance and which have not been updated at the port of entry shall be clearly identified so that they may be updated at the next available time.

4.3.4. In transport from port of entry to dealer

FR-OTA: 3-004.1

When a update of performance is officially announced, all vehicles in a market where the update of performance is to be made that are in transport from the port of entry to the dealer shall be clearly identified in the manufacturer's vehicle database by the OTAMG so that they can be updated when they arrive to the dealer.

FR-OTA: 3-004.2

Since connectivity to a cellular or Wi-Fi network cannot be guaranteed while a vehicle is being transported, no attempt shall be made to update a vehicle's ECU(s) during the time a vehicle is in transport.

4.3.5. At dealer

4.3.5.1 Prior to per-delivery inspection

FR-OTA: 3-005.1.1 - When an update of performance is officially announced, all vehicles in a market where the update of performance is to be made that have not had the update made prior to arrival at a dealer shall be identified and made ready for the required update during the pre-delivery inspection process.

4.3.5.2 Post pre-delivery inspection

FR-OTA: 1-005.1.2.1 - When an update of performance is officially announced, all vehicles in a market where the update of performance is to be made that have not had the update made prior to the pre-delivery inspection process shall, at the discretion of the dealer, have the affected ECU(s) updated during the pre-delivery inspection process.

FR-OTA: 1-005.1.2.2 - ECU(s) affected by an update of performance may be updated during the pre-delivery inspection process by the manufacturer's standard methods used in its authorized workshops. One method is to physically connect a vehicle to a workshop system, perform the update and confirm that the update has been properly made and no other ECU(s) or vehicle systems have been affected. Alternatively, a vehicle manufacturer may determine that vehicles affected by an update of performance may be updated in the workshop using OTA processes.

FR-OTA: 1-005.1.2.3 - When OTA processes are used to update the affected ECU(s), dealer personnel shall ensure the following:

FR-OTA: 1-005.1.2.3.1 - The vehicle has the necessary connectivity to a cellular wireless or Wi-Fi network during the required time for the update to be completed.

FR-OTA: 1-005.1.2.3.2 - The vehicle has the necessary battery life to allow the vehicle to complete the update.

FR-OTA: 1-005.1.2.3.3 - A confirmation is obtained that the update to the affected ECU(s) has been successfully completed.

FR-OTA: 1-005.1.2.3.4 - A confirmation is obtained that the update has not affected any other ECU(s) or vehicle functions.

4.3.5.3 Demonstration mode

FR-OTA: 1-005.1.3.1 - When an update of performance is officially announced, all vehicles in a market where the update of performance is to be made, and are being used for demonstration purposes, shall have the update made at the discretion of the dealer.

FR-OTA: 1-005.1.3.2 - If the update is made using OTA, the conditions listed in FR-OTA: 1-005.1.2.3 shall apply.

4.3.5.4 Post sale prior to delivery

FR-OTA: 3-005.4.1.1 - When an update of performance is officially announced, all vehicles in a market where the update of performance is to be made, and that have been sold to a customer, but have not yet been delivered to a customer, shall have the update made immediately.

FR-OTA: 3-005.4.1.2 - If the update is made using OTA, the conditions listed in FR-OTA: 3-005.1.2.3 shall apply.

4.3.6. At registered owner's or authorized driver's residence

FR-OTA: 3-006.1

An authorized driver or registered owner of a vehicle should be notified of an update of performance by the vehicle manufacturer within a 'reasonable time' after the final decision has been taken to initiate an update of performance.

FR-OTA: 3-006.1.1 – The OEM shall prepare a set of guidelines on how customers shall be notified of an update of performance.

FR-OTA: 3-006.1.2 - An update of performance notice may be sent to the vehicle for display on the vehicle's head unit as a substitute for or alternative to the recommended notification method unless this method is explicitly disallowed by the applicable regulations in the jurisdiction where the update of performance has been made.

FR-OTA: 3-006.2

Obtain authorization from the authorized driver or registered owner of the vehicle to perform the update of performance update.

FR-OTA: 3-006.2.1 – If the vehicle is brought to a dealer, the act of bringing the vehicle to the dealer and registering for the update shall constitute authorization.

FR-OTA: 3-006.2.2 – If the vehicle is not brought to a dealer and the authorized driver or registered owner wishes to have the update performed using OTA, authorization must be provided in a manner that confirms acceptance of the OTA process and securely identifies that the confirmation is being provided by the authorized driver or registered owner.

FR-OTA: 3-006.3

Deliver instructions to the authorized driver or registered owner of the vehicle on how the update will be performed, what responsibilities he or she has prior to, during and after the update, and what to do in case the update is not successfully completed.

FR-OTA: 3-006.4

When OTA processes are used to update the affected ECU(s), the authorized driver or registered owner shall be instructed to ensure the following:

FR-OTA: 3-006.4.1 - The vehicle has the necessary connectivity to a

cellular wireless or Wi-Fi network during the required time for the update to be completed.

FR-OTA: 3-006.4.2 - The vehicle has the necessary battery life to allow the vehicle to complete the update.

FR-OTA: 3-006.4.3 - A confirmation is obtained that the update to the affected ECU(s) has been successfully completed.

FR-OTA: 3-006.4.4 - A confirmation is obtained that the update has not affected any other ECU(s) or vehicle functions.

4.3.7. During the driving cycle

4.3.7.1 Operating on road

FR-OTA: 3-007.1.1 – When an update of performance is officially announced, all vehicles in a market where the update of performance is to be made will be notified of the update of performance. This notification shall occur according to FR-OTA: 3-006.1.

FR-OTA: 3-007.1.2 – No update of a vehicle's ECU(s) affected by an update of performance shall be made during a driving cycle while the vehicle is operating on a road with the motor running.

4.3.7.2 Stationary on road

FR-OTA: 3-007.2.1 – No update of a vehicle's ECU(s) affected by an update of performance shall be made during a driving cycle while the vehicle is operating on a road with the motor running, including when the vehicle is stationery (e.g., stopped at a traffic light).

4.3.7.3 Parked along a road

FR-OTA: 3-007.3.1 – An update of a vehicle's ECU(s) affected by an update of performance may be made during a driving cycle while the vehicle is stationary and parked along a road if, and only if, the following conditions can be met:

FR-OTA: 3-007.3.1.1 - The vehicle has the necessary connectivity to a cellular wireless or Wi-Fi network during the required time for the update to be completed.

FR-OTA: 3-007.3.1.2 - The vehicle has the necessary battery life to allow the vehicle to complete the update.

FR-OTA: 3-007.3.1.3 - A confirmation is obtained that the update to the affected ECU(s) has been successfully completed.

FR-OTA: 3-007.3.1.4 - A confirmation is obtained that the update has not affected any other ECU(s) or vehicle functions.

FR-OTA: 3-007.3.2. - If the performance update is made using OTA, the conditions listed in FR-OTA: 3-005.1.2.3 shall apply

4.3.8. Stationary in parking garage or on parking lot

FR-OTA: 3-008.1

An update of a vehicle's ECU(s) affected by an update of performance may be made during a driving cycle while the vehicle is stationary and parked along a road if, and only if, the following conditions can be met:

FR-OTA: 3-008.1.1 - The vehicle has the necessary connectivity to a cellular wireless or Wi-Fi network during the required time for the update to be completed.

FR-OTA: 3-008.1.2 - The vehicle has the necessary battery life to allow the vehicle to complete the update.

FR-OTA: 3-008.1.3 - A confirmation is obtained that the update to the affected ECU(s) has been successfully completed.

FR-OTA: 3-008.1.4 - A confirmation is obtained that the update has not affected any other ECU(s) or vehicle functions.

FR-OTA: 3-008.2

If the performance update is made using OTA, the conditions listed in FR-OTA: 3-005.1.2.3 shall apply

4.3.9. Other locations

4.3.9.1 On a ferry

FR-OTA: 3-009.1.1 - Since connectivity to a cellular or Wi-Fi network cannot be guaranteed while a vehicle is on a ferry, no attempt shall be made to update a vehicle's ECU(s) during the time a vehicle is on a ferry.

4.3.9.2 Off road

FR-OTA: 3-009.2.1 - Since connectivity to a cellular or Wi-Fi network cannot be guaranteed while a vehicle is off road, no attempt shall be made to update a vehicle's ECU(s) during the time a vehicle is off road.

4.3.9.3 In storage (main battery disconnected)

FR-OTA: 3-009.3.1 - Since connectivity to a cellular or Wi-Fi network cannot be guaranteed while a vehicle is in storage, and no power is available to the vehicle, no attempt shall be made to update a vehicle's ECU(s) during the time a vehicle is in transport.

4.3.10. Re-delivery

4.3.10.1 Broken communications

FR-OTA: 3-010.1.1 – Failure of a performance update due to broken communications shall be repeated from the initiation of the notification of the update from the OTAMG.

FR-OTA: 3-010.1.2 – The authorized driver or registered owner shall decide

how many times the re-delivery will be repeated before taking other corrective action, including visiting an authorized workshop where the update may be performed in a closely managed environment.

4.3.10.2 Software failure

FR-OTA: 3-010.2.1 – Failure of a performance update due to software failure shall be repeated from the initiation of the notification of the update from the OTAMG.

FR-OTA: 3-010.2.2 – The authorized driver or registered owner shall decide how many times the re-delivery will be repeated before taking other corrective action, including visiting an authorized workshop where the update may be performed in a closely managed environment.

4.4.Security Risk Corrective Action

Requirements for a security risk corrective action are the same as those for a non-recall operation update (Section 4.2), with the following additions:

FR-OTA: 4-000.1

Notes: