VDA | QMC

Qualitäts Management Center
im Verband der Automobilindustrie

Quality Management in the Automotive Industry

Recall Management Using Over-the-Air Updates

Draft

1st edition, February 2020

Online download document

Recall Management Using Over-the-Air Updates

Draft 1st edition, February 2020

Online download document

ISSN 0943-9412
Release: Online document February 2020
English edition published in March 2020

Verband der Automobilindustrie e.V. (VDA)
Qualitäts Management Center (QMC)
Behrenstraße 35, 10117 Berlin

Overall production:
Henrich Druck + Medien GmbH
Schwanheimer Straße 110, 60528 Frankfurt am Main

Printed on chlorine-free bleached paper

Exclusion of liability

This VDA document represents a non-binding recommendation to be applied for the introduction and maintenance of QM systems.
This guideline is free for anyone to use.
Anyone who uses it must make sure that the guideline is used correctly.

This VDA document takes account of the state of knowledge and technology prevailing at the time of the respective issue. The use of the VDA Recommendations does not absolve anyone of responsibility for his/her own actions. Every user acts on his/her own responsibility. Liability on the part of the VDA and those involved in preparing VDA recommendations is excluded.

Anyone who comes across incorrect information or the possibility of an incorrect interpretation when using these VDA recommendations is requested to notify this immediately to the VDA.

Copyright protection

Translations

This document will also be published in other languages. Please contact VDA QMC for the most current respective status.

Table of contents

Preface **5**

1 Objective and scope **9**

2 Recall process using OTA updates **7**

3 Examples **6**

4 Glossary **6**

5 Appendix: BPMN 2.0 ..... **5**

Literature **6**

Preface

Regular software updates are an integral part of the service concept across industries in the digital world. This approach will continue to establish in the automotive industry as well. Service centers are already installing new software versions, be it for engine and transmission control or for the numerous driver assistance and other safety-related systems. As a result of the complex system architecture in modern vehicles with connected control units and system functions that can be carried out by the interaction of several control units, this type of updating is a particular challenge. Since a vehicle is a product with high safety requirements, a subsequent update may not adversely affect the high quality and testing standards.

Over-the-air (*OTA*) updates are a modern variation of wireless update delivery that makes it unnecessary to bring a vehicle into a service center. It is to be expected that the scope of OTA updates will increase considerably in connected vehicles. Moreover, the automotive industry will not want to do without the quick and flexible provision of updates especially when it comes to safety, product maintenance and possible addition of functions. Continuous and secure OTA updates, however, represent a challenge for the automotive industry due to technical, organizational and regulatory issues.

OTA updates are also an opportunity for recall management to implement safety-related and legally relevant corrective measures in a faster, more customer-friendly and efficient manner. To this end, it is necessary to ensure a reliable distribution of OTA updates from provision by development through to completed installation in vehicles. That is why procedures must also be defined for such cases when OTA updates were interrupted or not completed successfully or were rejected by update-authorized vehicle users.

This VDA document describes a recommendation for recall management using OTA updates in order to ensure product safety and conformity in case of product deviations in vehicles. This recommendation can be applied by vehicle manufacturers, suppliers and service providers who are involved in the process. The process descriptions are supplemented by sample applications. The objective of this document is to establish an industry-wide uniform communication basis and ensure that the minimum requirements for implementing a recall management system using OTA updates are generally understood.

1 Objective and scope

This VDA document provides recommendations relating to the OTA update process for vehicle recall. In other words, the updates under discussion here relate exclusively to the correction of deviations in the product integrity. Updates relating to general product maintenance or added functionality are, however, not taken into consideration here.

This VDA document looks at OTA updates starting with the provision of the released software through to reporting after installation in the vehicles. That includes checking the OTA capability of vehicles, defining relevant criteria and feedback relating to the installation results, among other things.

The production of properly released updates and their provision is presupposed here and thus not described. On the other hand, this document does take into account the checking of vehicles' OTA capability as part of software distribution, but not the vehicles' OTA capability as part of product development. Cyber security for the OTA update process is assumed and not taken into account here.

This VDA document has been prepared to be general so that it can be adapted for all markets and companies in the automotive industry and their supply chain. In addition to that, the statutory regulations applicable in the respective countries and regions must be observed with regard to product integrity and OTA updates.

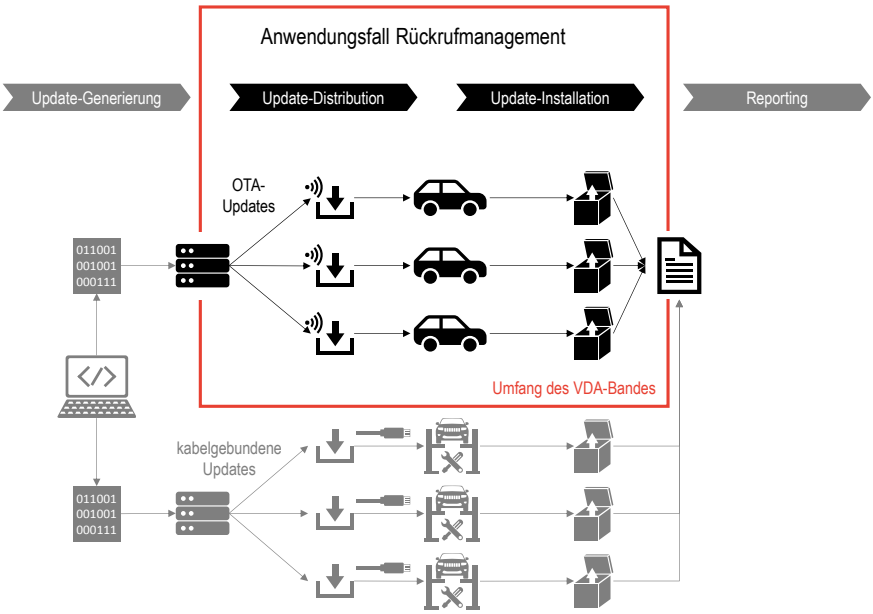

Figure 1: Scope and context of this VDA document

2 Recall process using OTA updates

According to the VDA document on product integrity, the product safety and conformity process consists of the following steps

1. Identifying product deviations,
2. Reporting product deviations internally,
3. Preparing an issue,
4. Making decisions,
5. Carrying out recall,
6. Analysis of effectiveness and
7. Lessons learned.[1]

With regard to the recall process using OTA updates, there are particular features for the process steps “Preparing an issue,” “Carrying out recall,” “Analysis of effectiveness” and “Lessons learned”; all other process steps remain unchanged and are not described any further here.

2.1 Preparing an issue

Preparing an issue for a possibly necessary product adaptation essentially includes an analysis of the circumstances. The following points must be taken into account if an OTA update is being considered as part of a defining measures step:

After identifying which vehicles are affected by the recall action, it is necessary to determine which of these vehicles are OTA-capable and thus eligible for an OTA update.

1 Cf. VDA document on “Product Integrity”, Section 4.4.

In this context, the technical, contractual and country-specific boundary conditions must be taken into account.

The operational state in which a vehicle must be (e.g. vehicle must be stationary, engine switched off, etc.) in order to be able to perform an OTA update should be noted and further specified if applicable. All prerequisites for carrying out a reliable OTA update must be fulfilled. In this context, the technical, contractual and country-specific boundary conditions must be taken into account.

As in the past, service centers must have access to updates with the same contents at the same time even in case of an OTA update. This is necessary in order to be able to provide updates to vehicles that are not OTA-capable, or in cases where update-authorized vehicle users prefer to visit a service center over an OTA update, or the OTA update could not be carried out successfully.

If the rejection of the update leads to an officially prescribed stoppage of vehicle operation, it is necessary to check whether vehicle user are to be informed in this regard as part of the request to update.

It must be considered how the vehicle may need to be configured after the installation of the OTA update and whether this would be feasible or reasonable for the vehicle user. (For instance, the window lifter may have to be programmed or initialized after an update and thus moved to the end stop.) Since this would have to be done by the vehicle user during an OTA update, such an OTA update could be impractical and therefore a wired update in a service center would be preferable.

2.2 Carrying out recall

As part of recall management, it is necessary to define whether and with which update rollouts which vehicles should get the update and

when and how to deal with updates that were not implemented. Legal, country-specific framework conditions must be taken into account and, if necessary, coordinated with the competent authorities.

The subsequent download and installation process for an individual vehicle is shown in Figure 2.2

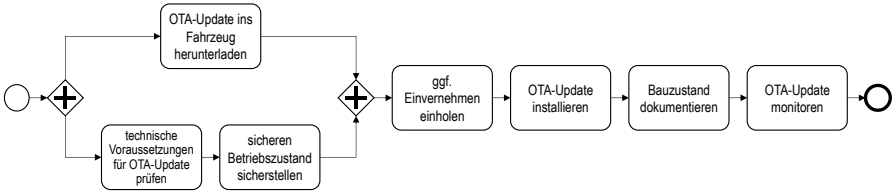

Figure 2: Process diagram of downloading and installation of OTA updates onto the vehicle

Prior to installing the OTA update, the update-authorized vehicle user must agree to the update.[3] Prior to agreeing to the installation, the update must be loaded onto the vehicle and the technical requirements and the safe operating condition must be checked.[4] After successful installation, the changed construction status is to be documented and the results of the update included in monitoring.

[2] The process is outlined in *Business Process Model Notation 2.0* (*BPMN 2.0*). A brief description of the notation used here can be found in the appendix (Section 0).

[3] Country-specific evaluations are to be performed to determine whether this has to be carried out separately for the specific update or whether it can be implemented in advance on the basis of general consent, e.g., as part of the terms of use.

[4] When generating the update or preparing the OTA action, it is necessary

Since OTA update or installations could not be completed successfully, the following points, among others, must be taken into account:

- Consideration of country-specific legal conditions for emergency operation or for vehicles with functional limitations and dealing with vehicles with limited driving ability
- Customer support during recall
- Monitoring and active control (if necessary, discontinuation) of recall

2.3 Analysis of effectiveness

Since a service center does not check the functionality of the vehicle or individual systems in the vehicle, particular attention is placed on field monitoring after installation of OTA updates.

During and after installation in individual vehicles, the authorities will be informed about the compliance rate in accordance with the country-specific requirements (possibly iteratively as well) and may be provided with any further information required.

2.4 Lessons learned

Deriving lessons learned[5] concludes the recall process. The following aspects may be of particular relevance for a recall using OTA updates:

[5] For implementing lessons learned, see VDA document on “Lessons Learned”

- User guidance during update (usability)
- Recall process management
- Installation strategy, hardware requirements, backward compatibility
- Verification of safe operating condition for installation process
- Causes for unsuccessful OTA updates

3 Examples

The following describes two recalls implemented using OTA updates. These descriptions are purely fictitious and thus provided only to illustrate. They are only used to highlight possible use cases and their implementation.

3.1 Example 1: Rearview camera software bug

Preparing the issue

An OEM has noticed that a software bug may cause the rearview camera image to be incomplete under certain operating conditions.

The analysis has revealed the following: There are 100,000 vehicles equipped with the corresponding software version, with 75,000 vehicles on the European market and 25,000 vehicles on the US market. On the US market, the rearview camera must display correctly according to relevant regulations, contrary to Europe. It is recommended to recall the 25,000 vehicles in the US as a result of the non-compliance with regulations while carrying out a quality measure for the 75,000 vehicles in Europe in order to avoid customer complaints.

Of the affected vehicles, 40,000 (28,000 in Europe, 12,000 in the US) are technically OTA-capable thanks to the hardware generation. The OEM determines the following conditions for installing the update: The vehicle must be safely parked, i.e. the doors are locked, automatic transmission placed in park, ignition switched off, the parking brake locked and there are sufficient resources for installing and then starting the vehicle by using the battery.

After the update, the vehicle user is not required to do any configuration or other activity, since the update results in a fully compliant and functioning operational state. Therefore, the recall in the US should be carried out for all 12,000 OTA-capable vehicles by using OTA. At

the same time, the service centers in the US must be supplied with updates for all 25,000 vehicles.

Vehicle users in the US are to be informed that the update is necessary in order to restore compliance with regulations. The information is displayed using release notes in the case of OTA updates. To confirm the update process, the vehicle user is informed that the vehicle cannot be operated during the update (for approx. 1 hour after parking the vehicle).

Carrying out recall

Approval to carry out the software updates must be obtained from the US authorities. 25,000 vehicles, of which 12,000 are OTA-capable, are included in the recall in the US. Breaking the recall down into update rollouts is not possible in the US due to the general legal framework.

For the 12,000 OTA-capable vehicles, the necessary software is downloaded during regular vehicle use. Interrupting the vehicle operation cycle does not abort the software download. Instead the download continues with the subsequent driving cycle. After the vehicle is parked and the update has been fully downloaded, the head unit will show that there is an update available for installation. The vehicle user must explicitly agree to the installation of the update, since the terms of use in this case do not include a general consent for updates.

After the update is successfully installed, the vehicle sends its updated construction status to the OEM's back-end system. This marks the vehicle as successfully updated in its recall system. When the competent authorities ask for information about the compliance rate, this information is evaluated and provided.

The procedure in Europe is similar for the 28,000 OTA-capable vehicles. With regard to user information, there is no reference to a non-conformity, since that is not the case here. It is not necessary to inform the authorities about the recall implementation and the compliance rate.

Analysis of effectiveness

Of the 12,000 OTA-capable vehicles affected in the US, 8,000 were successfully updated using OTA six months after the recalled started. 500 of the remaining 4,000 OTA-capable vehicles were successfully updated in service centers by the end of the same period. The vehicle users of the remaining 3,500 vehicles are prompted again to update.

Lessons learned

The installation process was estimated to take approx. 60 minutes, but actually took only about 20 minutes. This probably led to the small number of OTA updates. In the future, the indicated installation time should be estimated less conservatively.

3.2 Example 2: Cyber security vulnerability in the infotainment system

Preparing the issue

The operating software in the infotainment system has an open port and thus a cyber security vulnerability. Consequently, there is basically a possibility that malware may get onto the vehicle as a result of a cyber attack and simulate signals on the CAN bus. This could, for instance, adversely affect the engine control system.

There are 200,000 vehicles affected by the corresponding operating software worldwide. All of these vehicles are technically OTA-capable. In some markets, an OTA update is not possible due to legal restrictions or lack of the technical infrastructure. There are 20,000 vehicles affected in these markets, thus making the total of OTA-capable vehicles 180,000. A global recall is recommended as a result of the potential impact on the vehicles' safety-related control systems. The recall shall be carried out OTA.

The prerequisite for the installation is that the vehicle is safely parked. That means: the doors are locked, automatic transmission placed in park, ignition switched off, the parking brake locked and there are sufficient resources for installing and then starting the vehicle by using the battery.

At the same time, the service centers around the world are all supplied with the new software version. This is necessary, since some vehicles may not be reached using OTA, vehicle users could reject an OTA update or OTA updates could fail.

The vehicle user must be informed that the update is necessary in order to safeguard the requirements regarding cyber security. The information is displayed using release notes in the case of OTA updates. To confirm the update process, the vehicle user is informed that the vehicle cannot be operated during the installation (for approx. 1 hour after parking the vehicle).

After the update, the vehicle user is not required to do any configuration or other activity, since the update results in a fully compliant and functioning operational state.

Carrying out recall

All 200,000 vehicles are included in the recall program in one step, where 180,000 of them are OTA-update-capable.

The necessary software is downloaded during regular vehicle use. Interrupting the vehicle operation cycle does not abort the software download. Instead the download continues with the subsequent driving cycle. After the vehicle is parked and the update has been fully downloaded, the head unit will show that there is an update available for installation. The vehicle user must explicitly agree to the installation of the update, since the terms of use in this case do not include a general consent for updates.

After the update is successfully installed, the vehicle sends its updated construction status to the OEM's back-end system. This marks the vehicle as successfully updated in its recall system. When the competent authorities ask for information about the compliance rate, this information is evaluated and provided to the authority.

Analysis of effectiveness

Of the 180,000 OTA-capable vehicles affected, 150,000 were successfully updated using OTA six months after the recalled started. 12,000 of the remaining 30,000 OTA-capable vehicles were successfully updated in service centers by the end of the same period. The vehicle users of the remaining 18,000 vehicles are prompted again to update.

Lessons learned

There were five complaints during the first week of the recall, since the update did not go smoothly. The error remediation process identified the cause to be a hardware version of the infotainment system that was not verified for this OTA case in the recall scope. To remedy the situation, the missing hardware version was included in the software update of the affected vehicles. Lesson learned is to ensure that all affected hardware versions are recorded entirely and verified using a checklist system in the future.

4 Glossary

Operational state	The operational state is the operating mode which describes the current status of the vehicle. Examples are: which gear is engaged; the charging state of the battery; whether the doors and or lids are locked; the latching status of the (manual) hand brake.
Safe operating condition	The operating condition in which an OTA update can be performed. The safe operating condition is defined by the requirements from a specific campaign.
Cyber security	According to ISO/IEC 27032, cyber security is the “preservation of confidentiality, integrity and availability of information in the cyberspace”.
Vehicle user	The vehicle user is a person who has actual governance over a vehicle. This vehicle user can also be, but is not always, the registered owner (according to vehicle papers) or the actual owner.
Update-authorized vehicle user	The update-authorized vehicle user has the legal right to accept software updates for the vehicle in his/her possession.

Terms of use	The terms of use are the stipulations which regulate the use of online services and their associated options by the customer.
OTA-capability, OTA-capable	A vehicle is OTA-capable if both the technical and legal prerequisites (incl. applicable country-specific laws) for deployment of Over-the-Air updates are fulfilled.
OTA update	OTA update is a method of data transfer for updating software. As the name suggests, this process does not require a wire-connection to the vehicle.
Over-the-Air (OTA)	Over-the-Air (abbreviated OTA) is a technical, wireless option for data transmission.
Product deviation	A product deviation is a non-conformance of a product to valid regulations, laws and/or specifications. It represents a discrepancy versus the expected properties of a product.
Pproduct integrity	Product integrity encompasses product safety and product conformity. It is described in the VDA publication "Product Integrity" (VDA 2018).
Release notes	Release notes include information which is provided to a customer describing the content of an OTA update.
Recall management	Recall management is a management process which describes the organization of recalls of vehicles in customer hands in accordance with VDA publication "Product Integrity" (VDA 2018).

Software	Software is a collective term for programs and their associated data. Software can include executable programs (e.g. a program which controls an ECU), configuration files (e.g. the configuration of an ECU) and/or content (e.g. map data for a navigation system).
Update rollout	An update rollout includes the distribution and installation of OTA updates for a previously defined subset of vehicles, for which the OTA update is scheduled. A single campaign can consist of multiple update rollouts.

5 Appendix: BPMN 2.0

The Business Process Model Notation (BPMN) version 2.0 was used in this document to describe processes.
The following elements of this notation were used here:

Eine *Aufgabe* ist eine Arbeitseinheit.

Eine *Sequenzfluss* definiert die Abfolge der Ausführungen.

Ein *paralleles Gateway* markiert ein Aufteilen des Kontrollflusses in parallele Aktivitäten bzw. ein Zusammenführen verschiedener Zweige, die alle abgeschlossen sind.

Ein *Start* ist der Beginn eines Prozesses.

Ein *Ende* ist das Ende eines Prozesses.

Literature

UNECE (2018): Draft Recommendation on Software Updates of the Task Force on Cyber Security and Over-the-air issues, available at: https://www.unece.org/fileadmin/DAM/trans/doc/2019/wp29grva/ECE-TRANS-WP29-GRVA-2019-03e.pdf [accessed on Jun. 4, 2019].

VDA (2018): Product Integrity – Recommended action for organizations regarding product safety and conformity, 1st edition, November 2018

VDA (2018a): Lessons Learned – Definition von „Lessons Learned" in der Automobilindustrie. 1st edition, November 2018

Quality Management in the Automotive Industry

You can find the current status of the published VDA volumes on Quality Management in the Automotive Industry (QAI) on the Internet at http://www.vda-qmc.de.

You can also place direct orders on this homepage.

Reference:

Verband der Automobilindustrie e.V. (VDA)
Qualitäts Management Center (QMC)

Behrenstraße 35, 10117 Berlin
Telephone +49 (0) 30 -89 78 42235, Fax +49 (0) 30 -89 78 42605
e-mail: info@vda-qmc.de, Internet: