



Qualitäts Management Center
im Verband der Automobilindustrie

Quality Management in the Automotive Industry

Recall Management Using Over-the-Air Updates

1st edition, July 2020

Online download document

VDA | QMC

Qualitäts Management Center
im Verband der Automobilindustrie

汽车行业质量管理

召回管理使用

Over-the-Air 空中下载升级

第 1 版, 2020 年 7 月

在线下载文档

Recall Management Using Over-the-Air Updates

1st edition, July 2020

[Online download document](#)

召回管理使用

Over-the-Air 空中下载升级

第 1 版, 2020 年 7 月

在线下载文档

ISSN 0943-9412

Release: Online document July 2020

English edition published in July 2020

Copyright 2020 by

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

ISSN 0943-9412

发行: 2020 年 7 月在线文档

2020 年 7 月英文版本发布

2020 版权所有人

德国汽车工业联合会 (VDA)

质量管理中心 (QMC)

柏林, Behrenstraße 35, 邮编 10117

承印:

Henrich Druck + Medien GmbH

法兰克福, Schwanheimer Straße 110, 邮编 60528

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

This document is protected by copyright. Any use outside the strict limits of the copyright laws without the permission of the VDA is prohibited and punishable by law. This applies in particular to reproductions, translations, microfilming as well as storage and processing in electronic systems.

Translations

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

责任免除

该 VDA 标准代表了一项非约束性建议，适用于质量管理体系的建立和维护。

该指南中的方法和行动建议对任何人都是免费的。
使用它的任何人都必须确保正确使用该指南。

该 VDA 标准参考了截至标准出版日期以前的最新文献。实施该 VDA 标准行动建议的企业仍负有相应的使用责任，风险由企业自己承担。VDA 及该标准的所有撰写及制作者在任何情况下都不承担任何责任。

如果在使用 VDA 标准期间发现错误或可能的误解，则要求立即将这些信息告知给 VDA。

版权保护

该出版物受版权保护。未经 VDA 同意，违反版权法规定的使用者，特别是复制、翻译、以微缩胶片存储或在电子设备系统中储存或处理该标准者，将受到法律惩处。

翻译事宜

该出版物将译成多种语言发行。最新译文应联系 VDA QMC 获取。

Table of contents

Preface	4
1 Objective and scope.....	7
2 Recall process using OTA updates	9
3 Examples	14
4 Glossary	20
5 Appendix: BPMN 2.0	23
Literature	24

目录

前言.....	4
1 目标与范围.....	7
2 召回过程中使用 OTA 升级.....	9
3 案例.....	14
4 词汇表.....	20
5 附录: BPMN 2.0	23
参考文献.....	24

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

前言

定期的软件更新是数字世界各个行业服务理念不可或缺的一部分。在汽车行业中，这种方法也将持续应用。服务中心将为消费者安装新的软件版本，无论是用于发动机和变速箱控制，还是用于众多驾驶员辅助和其它与安全相关的系统。由于现代车辆具有复杂的系统架构、具有互相连接的控制单元和可以通过多个控制单元的交互来执行的系统功能，因此这种类型的更新是一种特殊的挑战。由于车辆是对安全性有较高要求的产品，因此后续软件更新不能对汽车的高质量水平和测试标准产生不利影响。

Over-the-air (OTA) 空中下载更新是无线更新交付的一种先进技术，而无需将车辆驶入服务中心。可以预计，将来智能网联汽车的 OTA 更新范围将会大大增加。当然，汽车行业不想没有快速而灵活的软件更新过程，尤其是在安全性、产品维护和可能增加功能等方面。但是，由于技术、组织和法规方面的问题，持续且安全的 OTA 更新对汽车行业构成了挑战。

OTA 更新也为召回管理提供了机会，为有效的实施与安全和法律法规相关的纠正措施提供了更快捷、更加客户友好的方式。为此，有必要确保 OTA 更新的可靠分发，包括从开发提供到完整安装到车辆中。这就是为什么还必须为 OTA 更新中断、未成功完成或被最新升级授权的车辆用户拒绝的情况定义程序的原因。

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.

此 VDA 标准介绍了有关使用 OTA 更新进行召回管理的建议，以确保在车辆出现产品偏差情况下的产品安全性和符合性。参与该过程的车辆制造商、供应商和服务提供商可以应用此建议。同时应用案例对过程描述进行了补充介绍。本标准的目的是建立行业范围内统一的沟通基础，并确保对在召回管理系统中使用 OTA 更新的最低要求被广泛理解。

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.

1 目标与范围

该 VDA 标准提供了有关车辆召回中使用 OTA 升级的建议。换句话说，此处讨论的升级仅涉及产品诚信偏差的纠正处理。但是，此处不考虑与产品常规维护或附加功能有关的更新。

该 VDA 标准着眼于 OTA 更新，从提供已发布的软件一直到成功安装到车辆上为止。这包括检查车辆的 OTA 功能，定义相关标准以及与安装结果有关的反馈。

正确的发布更新及其提供在此处是预先假设的，因此不再描述。另一方面，此文档确实将检查车辆的 OTA 功能作为软件分发的一部分，但没有考虑车辆的 OTA 功能作为产品开发的一部分。另外，此处假设并没有考虑 OTA 更新过程中的网络安全性。

该 VDA 标准具有通用性，不仅适用于汽车行业，同时适用于所有相关行业及其供应链。除此之外，还必须遵守各个国家和地区适用的法律法规，以确保产品诚信和 OTA 更新。

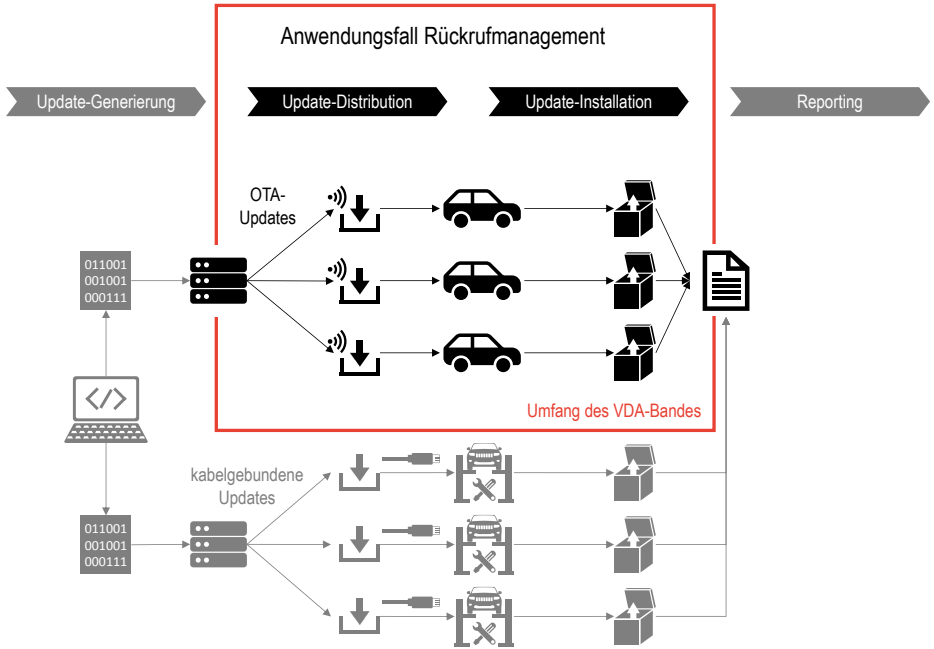


Figure 2: Scope and context of this VDA Volume

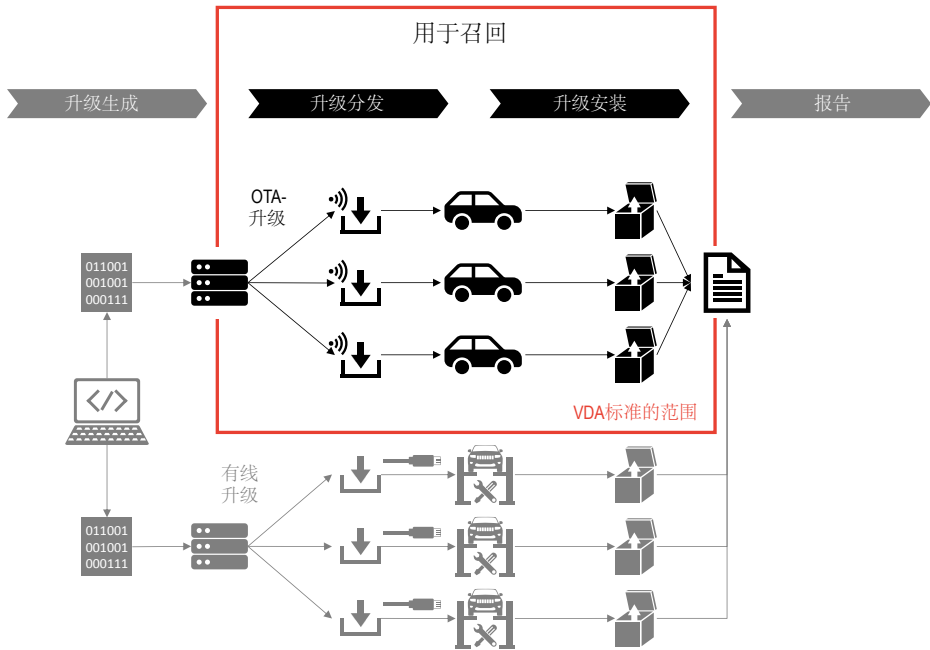


图 1：VDA 标准的范围与内容

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 Volume “Product Integrity”, Section 4.4.

2 召回过程中使用OTA升级

根据 VDA产品诚信标准，产品安全性和符合性流程包括以下步骤

1. 发现产品风险
2. 内部报告产品风险
3. 问题准备
4. 决策
5. 执行召回
6. 有效性验证
7. 经验教训总结。¹

关于召回过程中使用 OTA 升级，过程步骤“问题准备”，“执行召回”，“有效性验证”和“经验教训总结”具有特殊性；其它过程步骤均保持不变，此标准不再赘述。

2.1 问题准备

为可能的适用产品进行问题准备，本质上包括对问题的分析。如果将 OTA 升级视为定义措施步骤的一部分，则必须考虑以下几点：

在确定受到召回行动影响的范围后，有必要确定哪些车辆具有 OTA 功能，和可以进行 OTA 升级。

¹ Cf. VDA 产品诚信标准, 4.4 章节。

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 users 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

在这种情况下，必须考虑技术、合同和特定国家地区的要求。

为了能够顺利进行 OTA 升级，如果适用，还应进一步说明必要的满足执行 OTA 升级的所有先决条件。如车辆必须处于何种操作状态（例如：车辆必须处于静止状态，发动机关闭等）。在这种情况下，必须考虑技术、合同和特定国家/地区的法律法规要求。

与以往一样，即使可以 OTA 升级，服务中心也必须能够同时进行内容相同的升级。为了能够向不具备 OTA 功能的车辆提供升级，或者经过升级授权的车辆用户更喜欢到服务中心进行升级而不是通过 OTA，或者应对无法成功进行 OTA 升级的情况，这是必需的。

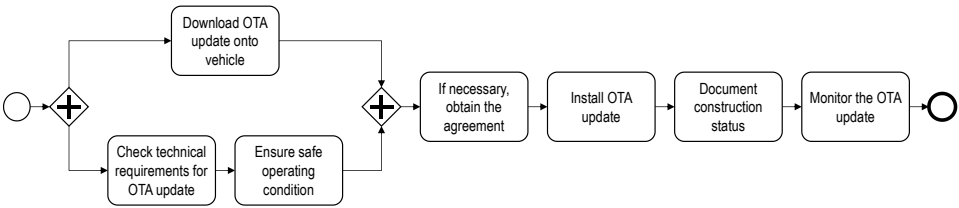
如果不能及时升级将导致车辆停止运行，则有必要检查是否将此作为升级请求的一部分通知车辆使用者。

必须考虑在安装 OTA 升级后可能需要如何配置车辆，以及这对于车辆用户是否可行或合理。（例如，玻璃升降器必须在升级后进行编程或初始化，然后移至终点挡块。）由于这必须由车辆用户在 OTA 升级期间完成，因此 OTA 升级可能不切实际，所以最好在服务中心进行对应更新活动。

2.2 执行召回

作为召回管理的一部分，有必要定义是否需要升级，使用哪种方式进行升级发布，哪些车辆应该被升级，以及何时、如何处理未实施的升级车辆。

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  3.²

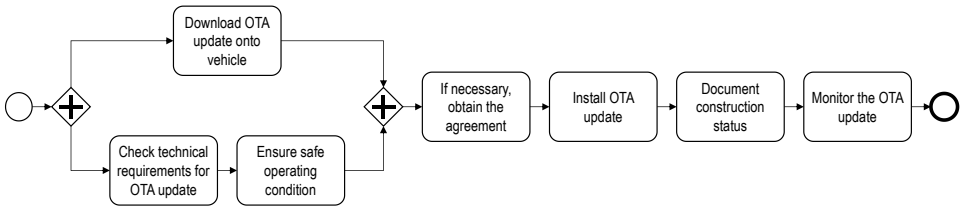


Figure 4: Process diagram of downloading and installation of OTA updates onto the vehicle

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 must be ensured that the download of the updates meets the IT security requirements.

必须考虑特定国家的法律法规要求，并在必要时与主管当局进行协调。

单个车辆的后续下载和安装过程如图 2² 所示。

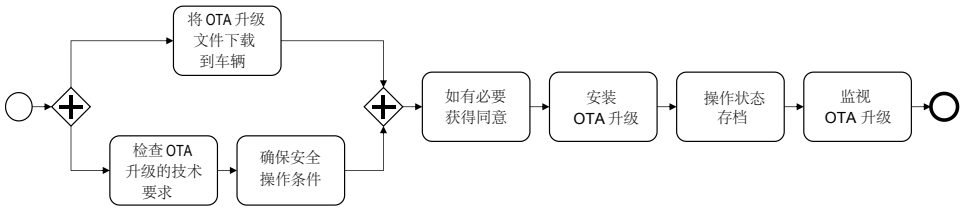


图 3： 汽车下载和安装 OTA 升级的流程图

在安装 OTA 升级之前，获得升级授权车辆的用户必须同意该升级³。在同意安装之前，必须将最新的数据包下载到车辆上，并且检查⁴技术要求和安全操作条件。成功安装后，应记录更改后的配置状况，并监视升级的结果。

² 业务流程模型表示法 2.0 (BPMN 2.0) 中概述了该流程。附录 (第 0 节) 中提供了此处使用符号的简要说明。

³ 应进行针对特定国家/地区的评估，以确定是否必须针对特定升级单独进行此评估，或者是否可以在普遍同意的基础上 (例如，作为使用条款的一部分) 提前实施该评估。

⁴ 在生成升级或准备 OTA 操作时，必须确保下载的升级符合 IT 安全要求。

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.

由于 OTA 更新或安装可能无法成功完成，因此必须考虑以下几点：

- 考虑针对紧急操作或功能受限的车辆以及处理驾驶能力有限的车辆的特定国家法律要求
- 召回期间的客户支持
- 监视和主动控制（必要时终止）召回

2.3 有效性验证

由于服务中心不检查车辆或车辆中各个系统的功能，因此在安装 OTA 升级后应特别注意现场监视。

在单独车辆安装期间和之后，将根据国家/地区特定要求（可能也是迭代的方式）向当局汇报完成率，并可能会提供所需的任何其它信息。

2.4 Lessons learned

Deriving lessons learned⁵ concludes the recall process. The following aspects may be of particular relevance for a recall using OTA updates:

- 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

⁵ For implementing lessons learned, see VDA Volume “Lessons Learned”.

2.4 经验教训总结

召回过程结束后应进行经验教训总结⁵。以下方面可能与召回中使用 OTA 升级特别相关：

- 更新期间的用户指南（可用性）
- 召回流程管理
- 安装策略，硬件要求，反向兼容性
- 验证安装过程的安全操作条件
- OTA 升级失败的原因

⁵ 执行经验教训总结,可以参见 VDA 经验教训标准。

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

3 案例

下面介绍使用 OTA 升级实现召回的两个案例。这些描述是虚构的，仅用于说明。它们仅用于强调可能的应用案例及其实现。

3.1 案例1：后视镜摄像头软件错误

问题准备

OEM 已经注意到，在某些操作条件下，软件错误可能导致后视镜摄像头图像不完整。

分析表明：有 100,000 辆汽车配备了相应的软件版本，其中欧洲市场有 75,000 辆，美国市场有 25,000 辆。在美国市场，后视镜摄像头必须按照相关规定正确显示，这与欧洲相反。由于不符合法规，建议在美国召回 25,000 辆汽车，同时对欧洲市场的 75,000 辆汽车进行质量评估，以避免客户投诉。

在受影响的车辆中，有 40,000 辆（在欧洲为 28,000 辆，在美国为 12,000 辆）基于硬件的版本不同，在技术上使用 OTA 进行软件升级是可行的。OEM 确定安装升级的运行条件如下：必须安全停放车辆，同时车门已锁好；自动变速箱已停驻，点火开关已关闭，驻车制动器已锁止，并且有足够的电池电量资源来安装和通过使用电池来启动车辆。

更新后，车辆用户无需进行任何配置或其它操作，因为升级后车辆具有完全合规性，并且可以达到功能完备的可操作状态。因此，应使用 OTA 对所有 12,000 辆具有 OTA 功能的车辆进行召回。

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.

同时，必须为美国的服务中心提供所有 25,000 辆汽车的升级服务准备。

美国的车辆用户将被告知必须进行升级才能符合法规要求。如果采用 OTA 升级，则使用发布的升级说明来显示该信息。为了确认升级过程，车辆用户被告知在升级期间（在停放车辆后约 1 个小时内）无法操作车辆。

执行召回

必须从美国当局获得批准以进行软件升级。在美国的召回中包括 25,000 辆汽车，其中 12,000 辆具有 OTA 功能。由于普遍的法律框架，在美国无法将召回分批次进行。

对于支持 OTA 的 12,000 辆汽车，在车辆常规使用期间会下载必要的软件升级包。中断车辆运行不会中止软件下载。取而代之的是，车辆运行后，下载将继续。车辆停放并且完全下载了升级文件后，主机将显示有可供安装的升级文件。车辆用户必须明确同意安装升级，因为在使用条款中并不包含用户接受自动升级的条款。

成功安装升级后，车辆会将其升级的配置状态发送到 OEM 的后台系统。这标志着车辆已在其召回系统中成功升级。当主管部门要求提供有关完成率的信息时，将评估并提供此信息。

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.

在欧洲，对 28,000 辆支持 OTA 的车辆采用类似的升级程序。由于没有对应的法规要求，因此这里的情况不同。没必要通知当局有关召回的实施情况和完成率等信息。

有效性验证

在召回开始六个月后，在美国受影响的 12,000 辆支持 OTA 的车辆中，有 8,000 辆使用 OTA 成功升级。在同一时期结束时，在服务中心成功更新了剩余的 4,000 辆具有 OTA 功能的车辆中的 500 辆。剩余 3,500 辆车的车主再次被提示升级。

经验教训总结

前期估计升级安装过程大约需要花费时间 60 分钟，但实际上只花了大约 20 分钟。这可能是导致 OTA 升级的车辆数量较少的原因。将来，不应过于保守地估计安装时间。

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).

3.2 案例 2: 信息娱乐系统的网络安全漏洞

问题准备

信息娱乐系统中的操作软件具有开放端口，因此存在网络安全漏洞。当受到网络攻击时，恶意软件可能会进入车辆并模拟 CAN 总线上的信号。例如，这可能会对发动机控制系统产生不利影响。

全球有 200,000 辆汽车受到相应操作软件的影响。所有这些车辆在技术上都支持 OTA。在某些市场中，由于法律限制或缺乏技术基础架构，无法进行 OTA 升级，在这些市场中有 20,000 辆汽车受到影响，因此，具备 OTA 升级条件的车辆总数为 180,000 辆。由于该漏洞可能会对车辆的安全相关控制系统造成潜在影响，因此建议进行全球召回。召回使用 OTA 进行。

安装升级包的前提条件是必须安全停放车辆。这意味着：车门已锁好，自动变速箱处于驻车状态，点火开关已关闭，驻车制动器已锁止，并且有足够的电池电量资源来安装升级包和使用电池启动车辆。

同时，世界各地的服务中心都必须提供了新的软件版本，因为某些车辆可能无法使用 OTA 升级，车辆用户可能会拒绝 OTA 升级，或者 OTA 升级可能会失败。

必须告知车辆用户进行升级的必要性，以确保符合有关网络安全的要求。如果是 OTA 升级，则使用发布的升级说明显示该信息。为了确保更新过程，在安装过程中（在停放车辆后约 1 个小时内）通知车辆使用者车辆无法操作。

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

升级后，车辆用户无需进行任何配置或其它操作，因为升级后车辆具有完全合规性，并且可以达到功能完备的可操作状态。

执行召回

计划所有 200,000 辆汽车同一批次进行召回，其中 180,000 辆具有 OTA 升级功能。

在常规车辆使用期间会下载必要的软件升级包。中断车辆运行不会中止软件下载。取而代之的是，在后续车辆运行时，下载将继续进行。车辆停放并且完全下载了升级文件后，主机将显示有可供安装的升级文件。车辆用户必须明确同意安装升级，因为在使用条款中并不包含用户接受自动升级的条款。

成功安装升级后，车辆会将其升级的配置状态发送到 OEM 的后台系统。这标志着车辆已在其召回系统中成功升级。当主管部门要求提供有关完成率的信息时，将评估此信息并将其提供给主管部门。

有效性分析

在召回开始六个月后，受影响的 180,000 辆支持 OTA 的车辆中，有 150,000 辆使用 OTA 成功升级。到同一时期结束时，在服务中心成功升级了剩余的 30,000 辆具有 OTA 功能的车辆中的 12,000 辆。剩余的 18,000 辆车的车主再次被提示升级。

经验教训总结

召回活动的第一周有五起由于升级不能自动完成的投诉。错误纠正过程将原因确定为信息娱乐系统的硬件版本无法识别，尚未在召回范围内对此 OTA 案例进行验证。

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.

为补救这种情况，检查丢失的硬件版本已包含在受影响车辆的软件更新中。经验教训是确保所有受影响的硬件版本都被完整地记录下来，并在将来使用检查表系统进行验证。

4 Glossary

<i>Cyber security</i>	According to ISO/IEC 27032, cyber security is the “preservation of confidentiality, integrity and availability of information in the cyberspace”.
<i>Operational state</i>	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.
<i>OTA-capability, OTA-capable</i>	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.
<i>OTA update</i>	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.
<i>Over-the-Air (OTA)</i>	Over-the-Air (abbreviated OTA) is a technical, wireless option for data transmission.
<i>Product deviation</i>	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.

4 词汇表

网络安全 根据 ISO / IEC 27032，网络安全是“保持网络空间中信息的机密性，完整性和可用性”。

操作状态 操作状态是描述车辆当前状态的操作模式。例如：档位状态；电池的充电状态；车门和盖是否锁紧；（手动）手刹的锁定状态。

具有 OTA 功能，OTA 可用 如果同时满足了使用 OTA 升级的技术和法律先决条件（包括适用于特定国家的法律），则该车辆具有 OTA 功能。

OTA 升级 OTA 升级是用于软件升级的数据传输方法。顾名思义，此过程不需要通过线束与车辆连接。

空中下载 (OTA) Over-the-Air 空中下载（缩写为 OTA）是一种用于无线数据传输的技术。

产品偏差 产品偏差是指产品不符合有效的法律、法规和/或规格。它表示与产品预期性能的差异。

<i>Product integrity</i>	Product integrity encompasses product safety and product conformity. It is described in the VDA publication "Product Integrity" (VDA 2018).
<i>Release notes</i>	Release notes include information which is provided to a customer describing the content of an OTA update.
<i>Recall management</i>	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).
<i>Safe operating condition</i>	The operating condition in which an OTA update can be performed. The safe operating condition is defined by the requirements from a specific campaign.
<i>Software</i>	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).
<i>Terms of use</i>	The terms of use are the stipulations which regulate the use of online services and their associated options by the customer.

产品诚信

产品诚信包括产品安全性和产品符合性。在 VDA 出版物“产品诚信”（2018版）中对此进行了描述。

召回管理

召回管理是一个管理过程，描述了根据 VDA 出版物“产品诚信”（2018 版）组织从客户手中召回车辆的过程。

发布升级说明

发布升级说明包括提供给客户的描述 OTA 升级内容的信息。

安全操作条件

可以执行 OTA 升级的操作条件。安全操作条件由特定活动的要求定义。

软件

软件是程序及其相关数据的统称。软件可以包括可执行程序（例如，控制 ECU 的程序），配置文件（例如，ECU 的配置）和/或内容（例如，导航系统的地图数据）。

使用条款

使用条款是规范客户对在线服务及其相关选项的使用的规定。

*Update-authorized
vehicle user*

The update-authorized vehicle user has the legal right to accept software updates for the vehicle in his/her possession.

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.

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.

升级授权的车辆用户

具有升级授权的车辆用户具有接受他/她拥有的车辆软件升级的合法权利。

升级发布

升级发布包括为先前定义的车辆集合分配和安装 OTA 升级，为此计划了 OTA 升级。单个战役可以包含多个升级发布。

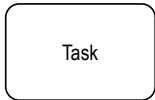
车辆用户

车辆用户是对车辆有实际控制权的人。该车辆用户也可以是（但并非总是）注册所有者（根据车辆文件）或实际所有者。

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:



A **task** is a unit of work.



A **sequence flow** defines the sequence of executions.



A **parallel gateway** marks a division of the control flow into parallel activities or a merging of different branches all completed.



A **start** is the beginning of a process.



An **end** is the end of a process.

5 附录: BPMN 2.0

本标准中使用了业务流程模型符号（Business Process Model Notation- BPMN）2.0 版来描述流程。

此标准使用了以下元素符号：



任务是工作的单位。



顺序流定义了执行顺序。



并行网关标志着将控制流划分为并行活动或所有已完成的不同分支的合并。



开始是一个过程的开始



结束是过程的结束。

Literature

UNECE (2020): *Draft new UN Regulation on uniform provisions concerning the approval of software update processes*. Retrieved from: <https://www.unece.org/fileadmin/DAM/trans/doc/2020/wp29grva/GRVA-05-06e.pdf>

VDA (2018): *Product Integrity. Recommended action for organizations regarding product safety and conformity* (1st ed.). Berlin, Germany: Verband der Automobilindustrie (VDA) e. V.

VDA (2018a): *Lessons Learned. Definition von Lessons Learned in der Automobilindustrie, Prozessbeschreibung, Anwendungstipps und Praxisbeispiele* (1st ed.). Berlin, Germany: Verband der Automobilindustrie (VDA) e. V.

参考文献

UNECE (2020): *联合国起草的关于批准软件更新程序的统一规定的新条例*。检索自:

<https://www.unece.org/fileadmin/DAM/trans/doc/2020/wp29grva/GRVA-05-06e.pdf>

VDA (2018): *产品诚信。组织产品安全与符合性行动建议* (第1版)。柏林, 德国: 德国汽车工业联合会 (VDA) e. V.

VDA (2018a): *经验教训。汽车行业经验教训的定义、过程说明、应用技巧和实践案例* (第1版)。柏林, 德国: 德国汽车工业联合会 (VDA) e. V.

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: www.vda-qmc.de

汽车工业质量管理

您可以通过 <http://www.vda-qmc.de> 网站查看已发布的 VDA 汽车工业质量管理 (QAI) 相关标准的最新状态。

您也可以直接在主页订购。

参考:

德国汽车工业联合会 e.V. (VDA)

质量管理中心 (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: www.vda-qmc.de

