ICS 43.020
CCS T 40

# DB4403

深　　圳　　市　　地　　方　　标　　准

DB4403/T XXX—XXXX

# 智能网联汽车软件升级技术要求

Technical requirements for software updates for intelligent and connected vehicles

（送审稿）

XXXX-XX-XX 发布　　XXXX-XX-XX 实施

深圳市市场监督管理局　发布

# 目　　次

# 前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件以强制性国家标准《汽车软件升级通用技术要求》征求意见稿（计划号：20214423-Q-339）（2022年6月版本）为基础制定，主要用于支持深圳市智能网联汽车准入管理工作的实施。

本文件由深圳市工业和信息化局提出并归口。

本文件起草单位：深圳市工业和信息化局。

# 智能网联汽车软件升级技术要求

## 1 范围

本文件规定了软件升级管理体系要求、汽车软件升级车辆要求、试验方法、车辆型式的变更和扩展、说明书。

本文件适用于M类、N类汽车，其他车辆类型可参照执行。

## 2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

强制性国家标准《汽车软件升级通用技术要求》征求意见稿（计划号：20214423-Q-339）（2022年6月版本）。

DB4403/T XXXX—XXXX 智能网联汽车整车信息安全技术要求

## 3 术语和定义

下列术语和定义适用于本文件。

3.1

**软件 software**

电子控制系统中由数字数据和指令组成的部分。

3.2

**软件升级 software update**

将某版本的软件（3.1）更新到新版本或更改配置参数的过程。

3.3

**软件识别码 software identification number**

由车辆制造商定义，用于表示与型式批准相关系统中软件（3.1）信息的专用标识符。

注：软件识别码不同于软件版本号。

3.4

**软件升级管理体系 software update management system**

为完成软件升级（3.2）而制定的一种规范组织的过程和程序的系统方法。

3.5

**在线升级 over-the-air update**

通过无线方式而不是使用电缆或其他本地连接进行数据传输的软件升级（3.2）。

3.6

**升级包 update package**

用于进行软件升级（3.2）的软件包。

3.7

**执行 execution**

安装和激活已下载升级包（3.6）的过程。

3.8

**安全状态 safe state**

当软件升级（3.2）中断或失败时，一种没有不合理风险的运行模式。

3.9

**完整性验证数据 integrity validation data**

用以检测数据中的错误或变化的值。

**示例：**校验值、哈希值等。

3.10

**系统 system**

用于实现功能的一组车辆部件和/或子系统。

3.11

**车辆用户 vehicle user**

操作、驾驶、拥有或管理车辆的人。

**示例：**车辆所有者，车队经理的授权代表或雇员，车辆制造商的授权代表或雇员、授权的技术人员。

## 4 软件升级管理体系要求

### 4.1 一般要求

4.1.1 车辆制造商应具备软件升级管理体系。

4.1.2 对于每次软件升级，车辆制造商应记录并安全存储 4.3 要求的相关信息，该信息应至少保存至车型停产后 10 年。

4.1.3 对于具有软件识别码的车型，车辆制造商应确保：

a) 该车型的每个软件识别码是唯一可识别的；

b) 当软件升级导致车型扩展或变更时，同步该车型的相应软件识别码的所有信息。

4.1.4 若车辆未存储软件识别码，车辆制造商应确保：

a) 声明该车型型式批准相关系统中所有电子控制单元(ECU)的软件版本信息；；

b) 对所声明软件版本进行软件升级时，同步更新 a）中的声明。

### 4.2 过程要求

4.2.1 应具备唯一地标识型式批准相关车辆系统所有初始和更新的软件版本信息（至少包括软件版本号和相应升级包的完整性验证数据）以及相关硬件部件的过程。

4.2.2 对于具有软件识别码的车型，应具备：

a) 在软件升级前后，具备能访问该车型软件识别码相关信息的过程；

b) 在软件升级后，能更新软件识别码相关信息的过程，至少更新所有相关软件的版本及完整性验证数据；

c) 能验证相关系统中软件版本与相关软件识别码中软件版本保持一致的过程。

4.2.3 应具备识别被升级系统与车辆其他系统之间相关性的过程。

4.2.4 应具备识别软件升级的目标车辆的过程。

4.2.5 在软件升级发布之前，应具备确认软件升级与目标车辆配置兼容性的过程，至少应评估目标车辆在软件升级发布之前最新已知软硬件配置，以确保其与升级包的兼容性。

4.2.6 应具备评估、识别和记录软件升级是否会影响型式批准相关系统的过程，至少应包括软件升级是否会影响受型式批准约束的参数或其他关键参数。

4.2.7 应具备评估、识别和记录软件升级是否会增加、更改或启用在型式批准时不存在或未启用的任何功能，或是否会更改、禁用标准法规中定义的任何其他参数或功能的过程，至少应包括：

a) 型式批准相关的信息条目是否需要修改；

b) 型式试验结果是否不再适用软件升级后的车辆；

c) 对车辆功能的修改是否影响车辆的型式批准结果。

4.2.8 应具备评估、识别和记录软件升级是否会影响任何车辆其他系统(该系统可能与车辆安全和持续运行有关)，或是否会增加或更改车辆注册登记时的功能的过程。

4.2.9 应具备通知车辆用户有关软件升级的过程。

### 4.3 信息记录要求

4.3.1 描述车辆制造商进行软件升级的过程，以及证明其符合性的相关标准的文件。

4.3.2 在软件升级前后，描述准入或认证相关系统的配置的文件，至少应包括系统的硬件、软件（包括软件版本）的唯一标识以及相关车辆或系统参数。

4.3.3 在软件升级前后，每个软件识别码应有一个可审核的记录用于描述所有相关的软件，至少应包括所有相关软件的版本及完整性验证数据。
4.3.4 应具备记录目标车辆并确认其配置与软件升级兼容性的文件。
4.3.5 应具备描述每次软件升级的信息的文件，至少包括：

a) 软件升级的目的；
b) 软件升级可能影响的车辆系统或功能；
c) b)中系统或功能是否与型式批准有关；
d) 对于 c）中与型式批准有关的系统或功能，软件升级是否影响其符合性；
e) 软件升级是否影响系统的任何型式批准相关参数；
f) 是否获得软件升级批准；
g) 执行软件升级的方法和先决条件；
h) 确认软件升级将安全可靠地进行；
i) 确认软件升级已经成功通过验证和确认程序。

### 4.4 安全相关要求

4.4.1 应具备保护升级包的过程，合理地防止其在执行前被篡改。
4.4.2 应保护软件升级全过程，合理地防止其受到损害，包括软件升级发布系统。
4.4.3 应确保验证和确认车辆软件的功能和代码的过程是适当的。
4.4.4 应具备处理软件升级突发事件的应急管理机制。

### 4.5 在线升级的附加要求

4.5.1 若在线升级是在车辆行驶过程中进行，车辆制造商应证明其具备有关过程和程序以确保该软件升级不会影响车辆安全。
4.5.2 当在线升级需要特定的技能或复杂操作时，车辆制造商应证明其具备有关过程和程序以确保只有在专业人员在场或执行该操作的情况下才能进行软件升级。

## 5 车辆要求

### 5.1 一般要求

5.1.1 应保护升级包的真实性和完整性，合理地防止其受到损害和无效软件升级。
5.1.2 当车辆存储软件识别码时，车辆应具备更新软件识别码的能力，每个软件识别码应能通过使用电子通信接口，至少通过标准接口(如 OBD 端口)，以标准化的方式易于读取。
5.1.3 当车辆未存储软件识别码时，车辆应具备更新软件版本的能力，与准入或认证相关系统的软件版本应能通过使用电子通信接口，至少通过标准接口(如 OBD 端口)，以标准化的方式易于读取。
5.1.4 应保护车辆上的软件识别码和/或软件版本免受篡改。

### 5.2 在线升级的附加要求

5.2.1 在每次执行软件升级前，应告知车辆用户有关软件升级的信息，至少应包括：

a) 目的（如，软件升级的重要性，以及是否与召回、安全等有关）；
b) 对于车辆功能的任何更改；
c) 完成软件升级的预期时间；
d) 执行软件升级期间任何可能无法使用的车辆功能；
e) 可能帮助车辆用户安全执行软件升级的任何说明。

5.2.2 在执行软件升级前，应得到车辆用户的确认。
5.2.3 在每次执行软件升级前，应确保车辆满足先决条件。
5.2.4 在每次执行软件升级前，应确保车辆有足够电量（包括可能恢复到以前版本或使车辆进入安全状态所需的电量）完成软件升级。
5.2.5 若执行软件升级可能影响车辆安全，在执行软件升级中，应通过技术手段确保车辆安全。
5.2.6 若执行软件升级可能影响驾驶安全，在执行软件升级中，至少应满足：

a） 确保车辆不能被驾驶；
b） 确保任何影响成功执行软件升级或影响车辆安全的车辆功能不能被使用。

5.2.7 在执行软件升级中，不应禁止车辆用户从车内解除车门锁止状态。

5.2.8 在执行软件升级后，车辆应：
a） 告知车辆用户升级的结果（成功或失败）；
b） 若成功，告知车辆用户实施的更新，以及更新车载电子用户手册（如果有）；
c） 若失败，告知车辆用户处理建议。

5.2.9 若软件升级失败或中断，应确保将系统恢复到以前的可用版本或将车辆置于安全状态。

## 6 试验方法

### 6.1 升级包真实性完整性试验

对于在线升级，按照DB4403/T XXXX—XXXXA.6.2.2开展试验，试验结果符合5.1.1的要求；对于离线升级，按照《智能网联汽车整车信息安全技术要求》A.6.3开展试验，试验结果符合5.1.1的要求。

### 6.2 软件识别码/软件版本更新及读取试验

软件识别码/软件版本更新及读取试验分为以下两种情况：
a） 当车辆存储软件识别码时，在执行软件升级前，使用市场上可获取的读取工具读取车辆中软件识别码并进行记录，使用与准入或认证相关的软件升级包（软件识别码与本车不同），成功执行软件升级并使用通用读取工具读取升级后的软件识别码并进行记录，试验结果符合5.1.2 的要求；
b） 当车辆不存储软件识别码时，在执行软件升级前，使用通用读取工具读取车辆中软件版本并进行记录，使用与准入或认证相关的软件升级包（软件版本与本车不同），成功执行软件升级并使用通用读取工具读取升级后的软件版本并进行记录，试验结果符合 5.1.3 的要求。

### 6.3 软件识别码/软件版本防篡改试验

按照DB4403/T XXXX—XXXXA.7.4开展试验，试验结果符合5.1.4的要求。

### 6.4 用户告知试验

在执行软件升级前，检查和记录告知用户的信息内容，试验结果符合5.2.1的要求。

### 6.5 用户确认试验

在执行软件升级前，检查并记录所提供的用户确认操作选项及相应操作结果，试验结果符合5.2.2的要求。

### 6.6 先决条件试验

分别使车辆处于满足和不满足先决条件的状态下，执行软件升级，检查并记录车辆软件升级执行结果，试验结果符合5.2.3的要求。

### 6.7 电量保障试验

在满足其他先决条件情况下，分别使车辆处于满足电量保障和不满足电量保障的状态下，执行软件升级，检查并记录车辆执行软件升级结果，试验结果符合5.2.4的要求。

### 6.8 车辆安全试验

根据可能影响车辆安全的软件升级项目清单开展相应试验，检查并记录软件升级结果及车辆状态，试验结果符合5.2.5的要求。

### 6.9 驾驶安全试验

根据可能影响驾驶安全的软件升级项目清单开展相应试验，在软件升级执行过程中，尝试将车辆置于行驶状态，检查并记录软件升级结果及车辆行驶状态，试验结果符合5.2.6中a）的要求；在软件

升级执行过程中，尝试使用可能影响软件升级成功执行或影响车辆安全的车辆功能，检查并记录软件升级结果及相应车辆功能状态，试验结果符合5.2.6中b）的要求。

### 6.10 车门防锁止试验

锁止车门并执行软件升级，在执行软件升级过程中，从车内解锁车门，记录车门解锁结果，试验结果符合5.2.7的要求。

### 6.11 结果告知试验

软件升级成功后，检查并记录结果告知信息，检查并记录车载电子用户手册（如果适用），试验结果符合5.2.8a）和b）的要求。

软件升级失败后，检查并记录结果告知信息和用户建议，试验结果符合5.2.8a）和c）的要求。

### 6.12 升级失败处理试验

在软件升级执行过程中，触发软件升级失败或中断，检查并记录车辆状态，试验结果符合5.2.9的要求。

## 7 车辆型式的变更和扩展

### 7.1 总则

按本文件通过型式检验的车型，其结果可扩展到符合7.2判定条件的其他车型。车型获得扩展后，此扩展车型不可再扩展到其他车型。

### 7.2 判定条件

7.2.1 整车生产企业相同。

7.2.2 使用的软件升级管理体系与第 4 章的相关内容未发生变更。

7.2.3 若有用于实现软件升级的电子控制系统，则其软硬件的版本相同，但在不影响软件升级的控制策略时允许软件版本不同。

7.2.4 能被软件升级的电子控制系统未新增。

7.2.5 升级包完整性和真实性的保护方式相同。

7.2.6 车辆是否存储软件识别码的情况相同。

7.2.7 软件识别码和/或软件版本在车辆上的存储位置相同。

7.2.8 读取和保护软件识别码和/或软件版本的方式相同。

7.2.9 告知车辆用户软件升级信息及结果的方式相同或增加。

7.2.10 电量保障技术措施相同。

7.2.11 软件升级中断或失败后的处理策略及安全状态相同。

## 8 说明书

具备软件升级功能的车辆，其产品说明书至少应包含：

a) “本车具备软件升级功能”等内容的说明；

b) 软件升级失败或中断后，车辆安全状态的说明；

c) 软件升级操作方法的说明。