ICS 43.020
T40

中华人民共和国国家标准

GB/T XXXXX—XXXX

电动汽车充电系统信息安全技术要求

Technical requirements for cybersecurity of electric vehicles charging system

（征求意见稿）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前　　言.....II
1 范围.....1
2 规范性引用文件.....1
3 术语与定义.....1
4 电动汽车充电系统车内系统信息安全架构.....2
4.1 信息安全架构.....2
4.2 信息安全目标.....2
5 车内充电系统信息安全技术要求.....2
5.1 硬件安全技术要求.....2
5.2 软件安全要求.....3
5.3 数据安全要求.....3
5.4 通信安全要求.....3
6 测试评价方法.....4
6.1 硬件安全测试要求.....4
6.2 软件安全测试要求.....4
6.3 数据安全测试要求.....5
6.4 通信安全测试要求.....6

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。

本文件由中华人民共和国工业和信息化部提出。

本文件由全国汽车标准化技术委员会（SAC/TC 114）归口。

本文件起草单位：

本文件主要起草人：

电动汽车充电系统信息安全技术要求

1 范围

本标准规定了电动汽车充电系统车内系统信息安全技术要求和测试评价方法；
本标准适用于电动汽车充电系统车内系统信息安全的防护设计、开发、测试和评估。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是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。

GB/T 18487.1 电动汽车传导充电系统 第1部分通用要求
GB/T 19596 电动汽车术语
GB/T 27930 电动汽车非车载传导式充电机与电池管理系统之间的通信协议
GB/T 29317 电动汽车充换电设施术语
GB/T 35273 信息安全技术 个人信息安全规范
GB/T XXXX-XXXX 汽车信息安全通用技术要求

3 术语与定义

GB/T 19596、GB/T 29317、GB/T 35273、GB/T 18487.1、GB/T XXXX-XXXX 界定的以及下列术语和定义适用于本文件。

3.1

车内充电系统 in-vehicle charging system

电动汽车车内，以充电为目的满足充电相关功能的系统。

注：根据充电方式不同，可能包含一个或多个车载控制器，例如电池管理系统（Battery Management System，简称BMS）、车载通信控制单元（In-Vehicle Unit,简称IVU）等。

3.2

身份鉴别 authentication

即身份确认，确定使用者身份的过程，从而确定是否具有对某种资源的访问和使用权限。

3.3

重要数据 important data

车内充电系统相关防护数据，包含个人敏感信息、安全重要参数等数据。

3.4

车辆对外通信 out-of-vehicle communication

车内充电系统与车辆外部的通信，包括传导式充电方式的CAN通信、PLC通信，非传导式充电方式的无线通信等。

3.5

车内通信 in-vehicle communication

车内充电系统自身各控制器间以及与车辆内电子电气系统的通信，包括基于CAN、CANFD、LIN、以太网等车辆内部的通信。

4 电动汽车充电系统车内系统信息安全架构

4.1 信息安全架构

车内充电系统信息安全由硬件安全、软件安全、数据安全和通信安全四部分组成，通信安全涉及车内通信安全和车辆对外通信安全。

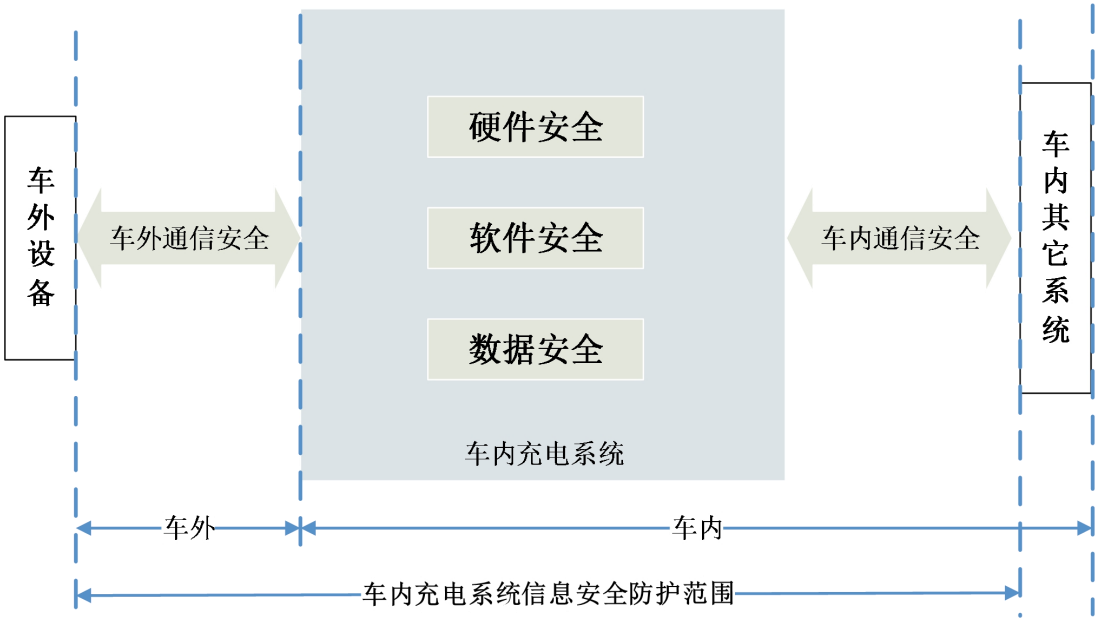

图 1 车内充电系统信息安全防护框架

4.2 信息安全目标

车内充电系统的信息安全目标是通过提出硬件、软件、数据和通信等方面的安全技术要求，防护车内充电系统面临的充电数据被窃取、个人隐私泄露和车内数据被窃取等风险。

注：对于受攻击有可能影响到自车以及其它车辆或系统的风险，车内充电系统中与外部充电装置直接进行通信的控制器应采取信息安全措施。对于车内充电系统其它控制器，可按主机厂要求的级别采取相应的信息安全措施。

5 车内充电系统信息安全技术要求

5.1 硬件安全技术要求

本项技术要求包括：

a) 车内充电系统所使用的关键芯片，如 MCU、加密芯片、通讯芯片等，宜采取必要的措施减少暴露管脚（例如采用 BGA/LGA 等封装的芯片）；
b) 应采取必要的措施保证车内充电系统的调试接口安全，如增加调试接口鉴权校验机制或禁止主板有调试接口暴露；
c) 直流充电通信 CAN 接口应满足 GB/T27930 中 4.3 定义（非车载充电机与 BMS 通信网络应由非车载充电机和 BMS 两个节点组成）。

5.2 软件安全要求

5.2.1 安全启动

车内充电系统软件启动时，应验证其完整性。

5.2.2 安全更新

本项技术要求包括：
a) 车内充电系统软件更新，应具有安全访问机制；
b) 车内充电系统软件更新，宜具有对升级程序文件进行完整性认证的机制（例如数字签名）。

5.2.3 安全日志

本项技术要求包括：
a) 车内充电系统的重要事件（如通信异常和安全启动失败等）宜生成日志，日志可存储在车内充电系统控制器上，也可借助车内其它系统（如车载终端）或车外系统（如车辆服务平台）存储日志；
b) 车内充电系统的日志应包含重要事件发生的流程信息（例如事件时间、事件类型和事件执行结果等）；
c) 应采取访问控制机制管理日志读取和写入的权限。

5.3 数据安全要求

5.3.1 数据完整性

车内充电系统存储的重要数据应具有完整性校验机制，当检测到重要数据在存储过程中完整性受到破坏时，应在检测到完整性错误时采取必要的异常数据处理机制（例如可恢复）。

5.3.2 数据保密性

车内充电系统存储的重要数据应进行加密保护，应保证存储区域的任何部分损坏或失效，以及非授权访问等不会导致重要数据的泄露。

5.4 通信安全要求

5.4.1 车辆对外通信安全

5.4.1.1 通信连接安全

车内充电系统在通信前若需进行认证（例如无线充电方式、即插即充功能）时，应具有身份鉴别机制，具有身份鉴别机制的车内充电系统对未识别身份的通信设备应终止通信连接。

5.4.1.2 通信传输安全

本项技术要求包括：

a) 车内充电系统传输的重要数据应使用密文传输，应保证该传输数据在被截获后无法得到明文数据；
b) 车内充电系统对重要数据的传输应采用完整性校验机制；
c) 车内充电系统对重要数据的传输应采用防重放机制。

5.4.1.3 通信接口安全

本项技术要求包括：

a) 的车辆对外通信接口应具有通信指令合法性验证机制，不应响应充电协议（如 GB / T 27930 标准协议）和主机厂规定协议之外的通信指令；
b) 车内充电系统的车辆对外通信接口不应具有访问车内通信总线数据的功能；
c) 直流充电通信 CAN 接口不应具有对车内充电系统以及车内其它系统进行控制器诊断、程序刷写和软件标定等操作功能（这些功能由 OBD 口执行）。

5.4.2 车内通信安全

车内充电系统自身各控制器以及车内其它控制器节点之间进行重要数据传输时，应使用安全机制确保传输重要数据的保密性、完整性和可用性。

6 测试评价方法

6.1 硬件安全测试要求

硬件安全的测试评价方法如下：

a) 测试方法
   1) 查阅芯片手册分析车内充电系统关键芯片是否采用 BGA/LGA 等封装；
   2) 分析评估是否存在暴露的调试接口；若存在，测试评估调试接口是否有鉴权校验机制；
   3) 查看测试样件（BMS 控制器）的直流充电通信 CAN 接口和车内 CAN 接口是否物理隔离，且连接通信网络的节点只有非车载充电机和 BMS 两个控制器。
b) 预期结果
   1) 车内充电系统关键芯片采用 BGA/LGA 等封装；
   2) 不存在暴露的调试接口，若存在，调试接口应具有鉴权校验机制；
   3) 测试样件（BMS 控制器）的直流充电通信 CAN 接口和车内 CAN 接口是物理隔离，且连接通信网络的节点只有非车载充电机和 BMS 两个控制器。
c) 结果判定
   上述预期结果均满足判定为符合，其它情况判定为不符合。

6.2 软件安全测试要求

6.2.1 安全启动

安全启动的测试评价方法如下：

a) 测试方法
   获取车内充电系统控制器正常运行的系统固件，使用软件调试工具对系统固件进行篡改，将破坏后的系统固件写入到车内充电系统控制器内的指定区域，监测车内充电系统控制器是否正常运行。

b） 预期结果

被篡改的系统固件在车内充电系统控制器上无法正常运行。

c） 结果判定

上述预期结果均满足判定为符合，其他情况皆判定为不符合。

6.2.2 安全更新

安全更新的测试评价方法如下：

a） 测试方法

1） 获取正常的升级流程，修改访问控制密钥，通过升级工具进行车内充电系统软件更新，检测升级流程过程中安全访问步骤是否通过，是否可正常更新；

2） 获取正确的升级程序文件，修改升级程序文件，通过升级工具进行车内充电系统软件更新，检测升级流程中是否对升级程序进行了完整性验证（例如：数字签名），是否可正常更新。

b） 预期结果

1） 升级流程中安全访问无法通过，无法更新车内充电系统软件；

2） 若升级过程中对升级程序文件进行了完整性验证，则无法更新车内充电系统软件。

c） 结果判定

上述预期结果均满足判定为符合，其他情况皆判定为不符合。

6.2.3 安全日志

安全日志的测试评价方法如下：

a） 测试方法：

1） 从记录日志的系统上读取日志，检查日志是否记录了需求的重要事件（如通信异常和安全启动失败等）；

2） 检查日志是否包含了事件发生的流程信息，例如事件时间、事件类型和事件执行结果等；

3） 检查日志访问的限制。

b） 预期结果：

1） 若有日志记录，日志记录包含了需求的重要事件；

2） 可以对每个事件进行完整的日志跟踪；

3） 日志访问会有权限控制。

c） 结果判定：

上述预计其结果均满足判定为符合，其他情况为不符合。

6.3 数据安全测试要求

6.3.1 数据完整性

数据完整性的测试评价方法如下：

a） 测试方法

使用软件调试工具通过调试接口合法认证访问车内充电系统重要数据存储地址，对存储的重要数据进行篡改，检测系统是否具有对存储数据的完整验证和保护机制。

b） 预期结果

车内充电系统在读取重要数据时，能够通过完整性验证识别被篡改的数据，并且可恢复被篡改的重要数据。

c） 结果判定

上述预期结果均满足判定为符合，其它情况判定为不符合。

6.3.2 数据保密性

数据保密性的测试评价方法如下：

a) 测试方法

使用软件调试工具通过调试接口合法认证访问车内充电系统重要数据存储地址，导出储存的重要数据。

b) 预期结果

导出的地址空间数据不能被解密出数据原始含义。

c) 结果判定

上述预期结果均满足判定为符合，其它情况判定为不符合。

6.4 通信安全测试要求

6.4.1 车外通信安全

6.4.1.1 通信连接安全

通信连接安全的测试评价方法如下：

a) 测试方法

测试具有身份鉴别机制的车内充电系统，将测试设备接入到系统通信网络中，向车内充电系统发送充电相关交互信息。

b) 预期结果

具有身份鉴别机制的车内充电系统对未识别身份的通信设备不会建立通信连接。

c) 结果判定

上述预期结果均满足判定为符合，其它情况判定为不符合。

6.4.1.2 通信传输安全

车外通信传输安全的测试评价方法如下：

a) 测试方法

1) 将测试设备接入车内充电系统所接车外通信网络，获取传输的数据，检测重要 数据是否以明文形式通过网络传输重要数据；
2) 将测试设备接入车内充电系统所接车外通信网络，发送被篡改、删除或插入的重要数据；
3) 将测试设备接入车内充电系统所接车外通信网络，采集重要数据传输过程的数据，然后重放之前采集的通信数据。

b) 预期结果

1) 车内充电系统通信接口不以明文形式通过网络传输重要数据；
2) 车内充电系统对完整性校验不通过的重要数据不响应；
3) 车内充电系统可识别重要数据为非法的重放数据，不做任何响应。

c) 结果判定

上述预期结果均满足判定为符合，其它情况判定为不符合。

6.4.1.3 通信接口安全

通信接口安全的测试评价方法如下：

a) 测试方法

1) 获取车内充电系统充电协议（如 GB / T 27930 标准协议）的样例数据和主机厂规定协议的样例数据，将测试设备接入车内充电系统所接车外通信网络，发送插入了非充电协议或非主机厂规定协议的样例数据，检查车内充电系统是否会响应充电协议和主机厂规定协议之外的通信指令；

2) 将测试设备接入车内充电系统所接车外通信网络，测试设备尝试通过车内充电系统的车外通信网络访问车内通信数据；

3) 获取车内充电系统控制器正常的诊断、程序刷写、标定样例数据，将测试设备接入直流充电通信 CAN 接口，发送诊断、刷写和标定样例数据。

b) 预期结果

1) 接收到非充电系统协议或非主机厂规定协议时不会响应；

2) 无法获取到任何车内通信数据；

3) 直流充电通信 CAN 接口进行诊断等操作功能的车内充电系统对诊断、刷写或标定不做任何响应。

c) 结果判定

上述预期结果均满足判定为符合，其它情况判定为不符合。

6.4.2 车内通信安全

车内通信传输安全的测试评价方法如下：

a) 测试方法

1) 将测试设备接入车内充电系统所接车内通信网络，获取传输的数据，检测重要数据是否以明文形式通过网络传输重要数据；

2) 将测试设备接入车内充电系统所接车内通信网络，发送被篡改、删除或插入的重要数据；

3) 将测试设备接入车内充电系统所接车内通信网络，采集重要数据传输过程的数据，然后重放之前采集的通信数据。

b) 预期结果

1） 车内充电系统通信接口不以明文形式通过网络传输重要数据；

2） 车内充电系统对完整性校验不通过的重要数据不响应；

3） 车内充电系统可识别重要数据为非法的重放数据，不做任何响应。

c) 结果判定

上述预期结果均满足判定为符合，其它情况判定为不符合。