推荐性国家标准

《电动汽车充电系统信息安全技术要求》

（征求意见稿）

编制说明

标准起草项目组

2020年9月

目录

《电动汽车充电系统信息安全技术要求》

（征求意见稿）

编制说明

一、 工作简况

（一）任务来源

本项目是根据国标委发[2019]22号文《国家标准化管理委员会关于下达第二批推荐性国家标准计划的通知》（计划项目编号20192313-T-339，标准项目名称《电动汽车充电系统信息安全技术要求》）进行制定，主要起草单位：xxxxxxxxxx等。

（二）工作过程

任务下达后，汽标委智能网联汽车分标委根据单位申请情况成立标准起草项目组，确定比亚迪汽车工业有限公司为牵头单位，并在此基础上明确了任务和分工，积极开展标准的研究、调研、起草、研讨等工作。

2018年05月～07月，标准项目启动预研，确定了标准制定的指导思想和原则，制定了标准的总体框架和工作计划。

2018年08月～12月，收集、整理并系统分析了电动汽车充电系统信息安全技术相关的法规、标准、文献资料等，开展了相关技术研究。

2019年01月～05月，经过标准起草项目组成员合理分工和反复讨论，完成标准草案技术要求部分。

2019年06月～11月，标准增加测试部分内容，形成完整版标准草案。

2019年07月，标准项目正式获批立项。

2019年12月～2020年03月，对标准草案组织专家进行了研讨和多次修改，形成工作组征求意见稿。

2020年04月～06月，面向汽车信息安全标准工作组广泛征求意见。

2020年07月～08月，根据工作组征求意见对标准草案进行修改完善，完善标准编制说明。

2020年08月，开展两轮标准试验验证工作，并根据试验数据讨论和完善标准文本。

2020年09月，完成标准公开征求意见稿。

1.项目组第一次会议

2018年5月22日，项目组在广州召开了“电动汽车充电系统信息安全技术要求国家标准编制项目组第一次会议”，正式启动标准制定工作。参会专家介绍了各自单位能够承担标准研究与制定项目相关工作等方面的情况，并对标准制定背景、标准适用范畴、标准基本内容、标准框架等进行了讨论并形成初步意见。

（1）标准草案讨论

- 项目框架范围

本项目主要对车载充电系统与充电设施（包含充电桩、充电站及其他）、车载充电系统与直连车身模块的数据和数据传输安全进行规范。同时，结合其他项目的框架范围，保证信息安全能够全面覆盖。

- 项目研究内容

项目重点对数据本身以及数据流传输的安全性提出技术要求，对传输方式（交流、直流、无线）不进行限定，但可对不同传输方式的安全提出不同安全级别的需求。

- 项目草案大纲

项目大纲包括三个方面：充电参数、认证健全和增值服务，再根据不同的应用场景（充电前、充电中、充电后）进行详细拆分。对充电系统中的数据流进行分析，确定纳入本标准的范围，并进行安全等级划分。

（2）下一步工作安排

- 比亚迪汽车工业有限公司牵头完善项目范围，其他参与单位反馈修改意见；
- 比亚迪汽车工业有限公司牵头草案大纲制定，其他参与单位反馈修改意见；

2.项目组第二次会议

2018年08月02日，在长春市，中汽中心组织标准牵头单位分别对《汽车信息安全通用技术要求》、《汽车网关信息安全技术要求》《电动汽车充电系统信息安全技术要求》《车载信息交互系统信息安全技术要求》《电动汽车远程服务与管理系统信息安全技术要求》进行工作汇报，梳理这五个标准的范围，确定标准的内容并对标准中涉及到的具体术语、标准结构、范畴及相互层级关系进行讨论。

（1）标准草案讨论

- 明确标准范围仅限于车与充电设施间的信息安全，不涉及云端（即桩企平台和车企平台）；
- 标准范围需要延伸至车内网络安全和外部设备接入时的车内总线安全,防止假冒的充电桩获取车内网络信息；
- 标准范围虽然不涉及云端，但是需要对诸如云端等系统提出边界要求；
- 标准的主体是明确技术指标及要求，并非详述具体加密算法。可以提出是硬件加密还是软件加密；
- 标准的聚焦点是现存的安全风险或问题，通过研究该类风险或问题的解决方案制定相关要求；
- 充电信息安全标准的核心在于车和桩之间的双向认证,需要引入密钥管理机制,实现密钥生成、密钥存储、更新等。

（2）下一步工作安排

- 依据其他企业针对《电动汽车充电系统信息安全技术要求》标准提出的意见，修改标准草案大纲，2018年9月1日前完成标准草案初稿。

3.项目组第三次会议

2018年10月23日,项目组在天津召开了“电动汽车充电系统信息安全技术要求国家标准编制项目组第三次会议”。本次会议针对第一版标准草案内容进行讨论，第一版标准草案涉及车载充电系统安全、车载充电系统和充电设备之间的通信安全、充电设备的系统安全、车载充电系统所接车内网络的安全。针对范围及内容进行了讨论。

（1）标准草案讨论

- 范围部分
  - 参考其他标准，应规范标准范围的描述；应指标准定义的技术要求所适用的范围。
- 规范性引用文件部分
  - 不可以引用低一级的标准。取消T/CEC 102.4,SZDB / Z 150.5—2015标准的引用，引用文件排序应该从小到大。
- 术语定义部分
  - 电动汽车充电系统术语改为车载充电系统；
  - 交流充电、直流充电术语定义不明确，重新定义；
  - 增加GB/T XXXX、GB/T XXXX和GB/T XXXX界定的以及下列术语和定义适用于本标准。
- 信息安全总体要求部分
  - 充电信息安全划分为设备安全、网络安全和数据安全；
  - 车载通信模块不纳入到安全范围。
- 信息安全技术要求部分
  - 按照设备安全、网络安全和数据安全三个方面进行信息安全技术要求；
  - 5.1.1中2）的描述改为应采用xx手段或技术，确保xx；
  - 5.1.1交流充电传输数据安全是基于附录A确定的信息安全技术要求；
  - 增加软件安全启动技术要求，在程序启动前验证软件的合法性，只有经过确认的合法软件才可以运行；
  - 不增加电动车充电信息安全测试相关内容，以后考虑作为测试标准；
  - 删除5.1.2 第5条。
- 附录部分
  - A.1占空比值增加误差范围定义；

- ✧ A.2不需要规定填充位、初始值的默认值；
- ✧ A.5 EBC改为ECB；
- ✧ A.8 不需要增加手机端支付时用户确认；
- ✧ A.9 车云平台改为桩云平台。

（2）下一步工作安排

- ➢ 按照会议中项目组各成员单位提出的建议修改本标准内容。——责任方：比亚迪；
- ➢ 目前标准没有规定具体的加密算法，是否规定具体的加密算法以及如何规定加密算法。——责任方：比亚迪；
- ➢ 提供充电过程中需加密保护的用户数据范围及具体项。时间是2018年10月31日前提供。——责任方：大众汽车（中国）投资有限公司；
- ➢ 确认电动汽车和充电设备之间数据传输安全部分内容的合理性，2018年10月31日前反馈至比亚迪——责任方：大众汽车（中国）投资有限公司；
- ➢ 列举充电过程中的信息安全风险项，并对风险项提出相应防护措施和技术要求，2018年10月31日前提供至比亚迪。——责任方：戴姆勒大中华区投资有限公司。

4.项目组第四次会议

2019年06月05日，项目组在无锡召开了“电动汽车充电系统信息安全技术要求国家标准编制项目组第四次会议”。标准的技术要求部分基本完成，本次会议主要由牵头单位组织项目组成员单位对该标准的技术要求部分进行回顾整理，会议过程中，对标准范围和标准内容进行了详细的讨论，会议明确了标准范围不涉及充电设备；并对标准内容逐一讨论，讨论技术要求是否合理及描述是否准确。秘书处提出技术标准需加入测试方法，因此本次会议对标准信息安全技术要求测试方法编写进行了任务分工。

（1）标准草案讨论

- ➢ 章节1范围：重新描述这部分内容；
- ➢ 章节2术语与定义：修改术语定义；
- ➢ 删除章节4.2，不需要写明具体的通信方式；
- ➢ 删除章节4.3，若需要定义，放到术语定义中；
- ➢ 信息安全技术要求以硬件安全、软件安全、数据安全和网络完全进行划分；
- ➢ 因为不能限制技术路线，所以不写具体采用的认证、加密、校验技术；
- ➢ 章节5.1.2.4内容修改为：电动汽车充电系统如果能够产生随机数，应能够产生安全的随机数；
- ➢ 删除章节5.2.1.1交流充电信息传输安全，因GB/T18487标准中未定义交流协议；
- ➢ 保留直流充电信息安全，GB/T27930现有协议内容无需加密，但应考虑前瞻性，考虑未来新增

数据；

- 本标准是否包含无线充电数据传输的安全，还需下次会议再确认；
- 章节5.2.2.5中删除OBD口要求，因已有OBD信息安全的相关标准正在起草；
- 删除附录A，因为附录A增加了交流充电的协议，如果交流充电要增加充电协议，协议的制定应包含在GB/T18487.1范畴；
- 删除附录B，因附录B增加了直流充电的安全通信协议，如果要增加直流充电协议，协议的制定应包含在GB/T27930范畴。

（2）下一步工作安排

- 硬件安全：提供硬件信息安全技术要求和测试方法；——负责单位：北汽新能源
- 软件安全：提供软件信息安全技术要求和测试方法；——负责单位：梆梆安全
- 数据安全：提供测试方法；——负责单位：中汽中心
- 层级整理及内容；——负责单位：比亚迪
- 3.2至3.5术语定义；——负责单位：戴姆勒
- 电动汽车充电系统所接车外接口和电动汽车充电系统所接车内接口的信息安全:提供技术要求和测试方法；——负责单位：比亚迪
- 以上工作内容由各单位在6月20日前完成，并反馈至比亚迪，由比亚迪进行汇总编辑完整草案。
- 6月底，召集项目组成员以视频电话会议形式对标准草案进行讨论。
- 7月18日准备在西安召开项目组标准会议。

5.项目组第五次会议

2019年07月02日，项目组通过电话会议形式召开了“电动汽车充电系统信息安全技术要求国家标准编制项目组第五次会议”。标准的技术要求部分基本完成，本次会议主要由牵头单位组织项目组成员单位对该标准的技术要求部分进行回顾整理，针对标准反馈意见进行了详尽的讨论。

（1）标准草案讨论

- 术语“电动汽车充电系统”引用GB/T18487.1标准中定义；
- “供电接口”和“充电接口”引用GB/T18487.1标准中定义；
- 重新对4.1信息安全架构进行描述；
- 数据的存储安全不包含可用性，可用性采用的是签名技术，数据存储满足完整性和机密性即可；
- 5.1.3“充电系统的充电CAN接口”更改为“电动汽车充电系统的直流充电通信CAN接口”；
- 充电数据需要进行加密传输的话便需要HSM加密；
- 保留软件安全中安全技术要求、反逆向机制、完整性保护机制、安全加固机制、恶意代码防范机制、安全审计、内存安全保护机制、异常数据监测机制，随机数产生、身份鉴别、安全启动、安全更新等机制；
- 从电动汽车充电系统的系统性能角度来说不适合保留日志，但从保证充电过程信息安全角度来讲需要保留日志进行安全审计；
- 反逆向机制和安全加固机制不一样，安全加固是对代码漏洞、不安全的编码方式进行加固；
- 本标准和软件升级安全标准不冲突，软件升级安全是从整车角度进行要求，本标准从自身系统方面进行要求；
- “防重放攻击”改为“传输时效性”；
- 防火墙这部分不建议放入访问控制，访问控制是禁止未授权的访问，防火墙是对通信数据进行过滤或隔离。现在已有CAN收发器支持建立白名单机制；
- “总线监控”技术要求中删除“在检测异常总线数据时应主动告警并禁止充电”。

（2）下一步工作安排

- 7月6日标准修改完成，再次征求意见，2019年7月17日召开标准起草组讨论会议。

6.项目组第六次会议

2019年07月17日，项目组成员单位在西安召开了“电动汽车充电系统信息安全技术要求国家标准编制项目组第六次会议”。会议主要讨论了电动汽车充电过程中的协议安全以及测试部分等内容。

各企业对电动汽车充电系统信息安全是否涉及充电过程中的协议安全进行了详细的讨论。具体针对是否保留身份鉴别、传输完整性、传输机密性和传输时效性要求展开讨论，明确了对于无线充电系统这些技术要求仍是适用的；最后对标准测试内容进行了讨论，涉及到测试方法应写到什么程度，如何实施

等问题。

（1）标准草案讨论

- 涉及充电协议安全的部分内容先保留，如果后续和充电联标准冲突，可删除；
- 5.4.1删除“直流充电”定语；
- 如若保留5.4.1.1身份鉴别，描述上应增加 “即插即充”/“敏感数据”等界定词；
- 本标准范围不包含放电，因放电的技术路线还未明确，目前放电时并没有通信功能；
- 4.1信息安全架构图比较粗略，需重新修改，图应能体现车内车外部分；
- 5.1.1芯片安全中SE和HSM应有详细的定义，修改“对抗暴力破解”的描述；
- 修改6.2.1安全基本要求、6.2.2完整性保护机制和6.2.7内存安全保护机制中个别字眼的描述。

（2）下一步工作安排

标准现已基本完成技术要求和测试内容的编写，但有待修改完善，现对标准编写分工如下：

- 范围、3术语定义——戴姆勒；
- 信息安全架构——比亚迪；
- 5.1和6.1硬件安全（技术要和测试要求）——北汽新能源、国家汽车质量监督检验中心（襄阳）；
- 5.2和6.2软件安全（技术要和测试要求）——梆梆安全、中国软件评测中心；
- 5.3和6.3数据安全（技术要和测试要求）——中汽中心数据中心；
- 5.4.1和6.4.1网络安全：电动汽车充电系统车外通信接口的安全（技术要求和测试方法）——宝马（中国）、大众汽车（中国）；
- 5.4.2和6.4.2网络安全：电动汽车充电系统车内通信接口的安全（技术要求和测试方法）——比亚迪、大众汽车（中国）；
- 8月2日前反馈标准中需要修改完善的内容。

7.项目组第七次会议

2019年11月04日，项目组在杭州召开了“电动汽车充电系统信息安全技术要求国家标准编制项目组第七次会议”。 各企业首先对标准反馈意见中“后门”、“安全漏洞”、“逆向分析”、“代码审计”和“不同种类的恶意代码”等描述进行了详细讨论，讨论修改为具体化、可操作性、可执行性的描述；网络安全部分内容改为不涉及通信对象和通信协议的技术要求；在技术要求逐一讨论过程中，秘书处提出技术要求内容不能写目的、描述、陈述、解释性的内容，若需写此内容，可放在注中。

（1）标准草案讨论

- 标准范围包括乘用车和商用车；
- 2、5.1.2 b)“通信线路应尽量隐蔽”，删除“尽量”；

- 不对通信对象和通信协议提要求；网络安全部分“…和…之间”改为车内充电系统在“通信前”/“应具有”等描述；
- 删除“5.4.6总线防火墙”和“5.4.7总线监控”；
- 技术要求中不适合使用太多“宜”；
- 技术要求不应写“目的、描述、陈述、解释”性内容，若需写此内容，可放在注中。

（2）下一步工作安排

标准内容修改任务如下：

- 戴姆勒提出标准范围应该更具体，例如包含传导式充电和非传导式充电——具体描述请戴姆勒补充；
- 5.2.4、5.2.5、5.2.6和5.2.7中“以使软件具备有效的保护”、“以防止恶意代码入侵”、“以防止非法修改、非法访问及破坏”、“会发生异常并禁止执行代码，以防止从受保护的内存位置执行恶意代码”等描述，秘书处提出不是规范的写法，技术要求不应写“目的、描述、陈述、解释”性内容。每一条都应该是要求性的描述，可改为“应具有。。。能力”、“应能够。。。”；全文都有这样的描述——梆梆安全修改软件部分，北汽新能源修改硬件部分，比亚迪修改数据和网络部分；
- 5.3.2数据机密性中内容分条写；——负责单位：比亚迪；
- 6.1.2主板安全中“板内通信不易被窃听”，“不易被窃听”应有程度边界描述；——负责单位：北汽新能源；
- 5.2.1安全基本要求“b) 车内充电系统软件不应存在中国汽车行业漏洞共享平台（CAVD）、国家信息安全漏洞共享平台（CNVD）、中国国家信息安全漏洞库（CNNVD）、CVE、CNCVE等公开发布了6个月及以上的高危安全漏洞”，上汽提出很难满足6个月要求，描述能涵盖未来出台的汽车漏洞平台；——负责单位：梆梆安全；
- 5.2.10异常数据监测机制中“告警”，是否会被问到告警的方式，是否应具体化或删除；——负责单位：梆梆安全；
- 6.2.1安全基本要求测试方法，访谈无法客观判定是否满足技术要求，重新描述下；——负责单位：梆梆安全；
- 6.2.4安全加固机制，测试方法描述应该更加具体一些；——负责单位：梆梆安全；
- 6.2.5恶意代码防范机制，访谈无法客观判定是否满足技术要求，重新描述下；——负责单位：梆梆安全；
- 6.2.6安全审计机制，若不写“审计日志”的相关要求，则6.2.6的题目应该修改，对应测试部分内容也应修改；——负责单位：梆梆安全；

- 11月20日前反馈修改内容，于标准制定项目组内再次征集意见。11月底前召开电话会议，形成一致意见标准草案。

8.项目组第八次会议

2020年07月04日，项目组因疫情的影响以远程会议的方式召开了“电动汽车充电系统信息安全技术要求国家标准编制项目组第八次会议”。本次会议由牵头单位组织项目组专家对汽车信息安全工作组征求的意见进行讨论和决议，并对标准草案进行了讨论。

（1）标准草案讨论

- 术语：“个人隐私信息”改为“个人敏感信息”；删除“其它主机厂定义的数据”，因其不具有判断是否满足标准的准则；
- 术语：“可信根实体”代替“安全模块”，GB/T 37935-2019中已定义；
- 安全架构： “网络安全”改为“通信安全”；
- 安全架构：增加“注：对于受到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。”
- 硬件安全：直流充电通信CAN接口应满足GB/T27930中4.3定义（充电机与BMS通信网络应由充电机和BMS两个节点组成）；
- 硬件安全：删除主板安全，必要性不强，带来维修不便；
- 硬件安全：芯片安全中“密钥存储、通信认证等行为”改为“有安全重要参数使用行为”；

- 硬件安全：删除“a）若车内充电系统有安全重要参数使用行为,宜在硬件安全模块内进行”；
- 软件安全：删除完整性保护机制、安全加固机制、内存安全保护、随机数产生和唯一标识符，保留安全启动、安全更新和安全日志；
- 软件安全：安全启动部分，“应对升级程序进行数字签名验证”改为“应对升级程序进行合法性认证（例如：数字签名）”，不限制具体技术路线；
- 软件安全：安全启动部分，删除“a）车内充电系统应具有安全启动机制，系统开始运行前应进行硬件信息和软件信息一致性检查”；删除b)“宜使用基于硬件级的完整验证机制”；
- 软件安全：安全日志修改a)b)为“a）车内充电系统的重要事件（如充电异常、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）”；
- 数据安全：删除“备份和恢复”；
- 数据安全：只针对重要数据的存储安全做要求，对重要数据的处理不做要求，原文保持不变；
- 通信安全：原文未进行车内和车外划分，改为划分车外通信安全和车内通信安全；
- 通信安全：“车内充电系统在通信前宜具有身份鉴别机制,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不应响应” 改为“车内充电系统在通信前若需要进行认证（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”，增加了身份鉴别的前提条件；
- 通信安全：通信传输安全只针对“重要数据”做要求；
- 通信安全,测试部分“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响应”改为“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”；
- 通信安全：定义“车外通信”和“车内通信”两个术语。

（2）下一步工作安排

- 根据反馈意见，修改标准内容；
- 意见反馈单位对反馈意见处理结果有异议的，可继续进行讨论；
- 确认充电系统样件测试事宜。

9.汽车信息安全标准工作组征求意见情况

工作组征求意见稿发出后，共收到反馈意见145条，会议中针对反馈意见进行了分类讨论，从范围、术语、安全架构、硬件安全、软件安全、通信安全几个方面进行讨论；其中，采纳意见74条，部分采纳意见17条，不采纳意见10，其它意见（原文删除）44条。在此基础上对标准进行了修改，形成公开征求

意见稿。

（三）主要参加单位和工作组成员及其所做的工作等

本标准由xxxxxxx单位共同起草。在本标准的制定过程中，多次组织行业专家进行了研讨，得到了相关单位的支持、协助与配合，取得了大量建设性意见和建议。

二、 国家标准编制原则和确定国家标准主要内容

1.标准编制原则

综合标准制定前期调研成果，结合试验验证情况确定本标准制定的基本原则为：

1）项目组内企业对标准内容广泛征求意见，并在工作组会议上充分讨论；

2）起草过程充分考虑国内外现有相关标准的统一和协调；

3）标准充分考虑了汽车主机厂、汽车零部件厂商和信息安全解决方案提供商的意见，在不偏离国际和国内当前行业技术水平的基础上前瞻性地考虑技术发展方向；

4）适当考虑标准条款对电动汽车充电系统零部件的软硬件成本的影响。

编写格式：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》的规定进行编制。

2.标准主要内容说明

本标准主要由范围、术语和定义、电动汽车充电系统信息安全架构、车内充电系统信息安全技术要求及测试评价方法等内容组成，相关国际标准根据国内的具体情况，进行编制，具体内容如下：

2.1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。依据调研结果，本标准适用于乘用车和商用车。

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外通信安全。

2.2 术语和定义

标准的术语和定义参考了 GB/T 19596、GB/T 29317、GB/T 35273、GB/T 18487.1《中的部分术语和定义，并且和推荐性国家标准《汽车信息安全通用技术要求》等相关内容进行了统一。并对“车内充电系统”、“身份鉴别”、“重要数据”、“车内通信”、“车外通信”进行了标准化定义。

2.3 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对外通信安全。

2.4 技术要求和测试评价方法

2.4.1 技术要求

硬件安全从芯片封装、调试接口、总线隔离方面提出硬件方面的信息安全要求。其中芯片封装，考虑到硬件成本，技术要求为“宜”。

软件安全从安全启动、安全更新、安全日志提出软件方面的信息安全要求。

数据安全从车内充电系统存储的重要数据的完整性、保密性提出信息安全要求。防护的数据限定为重要数据。

通信安全从车外通信安全和车内通信安全提出信息安全要求。

5.4.1.1 是对具有身份鉴别机制的车内充电系统提出的信息安全要求。考虑到无线充电方式、即插即充功能会应用到身份鉴别。

5.4.1.2 是车外通信传输的安全要求，5.4.2 是车内通信传输的安全要求，传输数据要求限定为重要数据的传输应满足通信传输安全要求。

2.4.2 测试评价方法

根据文件“5.车内充电系统信息安全技术要求”中的各条技术要求，逐一对应提出了本部分测试方法。

三、 主要试验（或验证）情况分析

1.试验（或验证）情况概览

通过项目组、工作组意见反馈及讨论，对于现有交流充电的车内充电系统，因无通信功能，本标准不做要求；对于现有直流充电的车内充电系统，因其使用的通信协议（GB/T 27930）都是明文传输，所以本标准只有部分条款适用，见下表 1，无即插即充功能的 BMS 适用条款标注了“√”，不适用条款标注了“×”；有即插即充功能的 BMS 和无线充的 IVU 适用于本标准所有条款。

表 1 标准适用范围

序号	测试编号	样件		
		无即插即充功能的 BMS	有即插即充功能的 BMS	IVU
1	6.1a)1)	√	√	√
2	6.1a)2)	√	√	√
3	6.1a)3)	√	√	√
4	6.2.1a)	√	√	√
5	6.2.2a)1)	√	√	√
6	6.2.2a)2)	√	√	√

7	6.2.3a)1)	×	√	√
8	6.2.3a)2)	×	√	√
9	6.2.3a)3)	×	√	√
10	6.3.1a)	×	√	√
11	6.3.2a)	×	√	√
12	6.4.1.1a)	×	√	√
13	6.4.1.2a)1)	×	√	√
14	6.4.1.2a)2)	×	√	√
15	6.4.1.2a)3)	×	√	√
16	6.4.1.3a)1)	√	√	√
17	6.4.1.3a)2)	√	√	√
18	6.4.1.3a)3)	√	√	√
19	6.4.2a)1)	×	√	√
20	6.4.2a)2)	×	√	√
21	6.4.2a)3)	×	√	√

本次测试验证的样件为无即插即充功能的BMS，验证测试项为9项。

2.试验（或验证）具体情况

测试时间：2020年08月13日至2020年08月17日

测试样件：BMS控制器,见图1。

测试单位与地点：天津 中汽研汽车检验中心(天津)有限公司 17 号楼 2 楼实验室。

测试工工具：数字视频展示台：用于硬件检查，可将样品图像进行放大，检查 PCB 板、芯片；

测试电脑：用于连接控制台，对样品进行测试及结果观察；

测试软件工具：对样品操作系统、应用软件、数据存储等进行测试分析；

直流电源、示波器等：辅助测试；

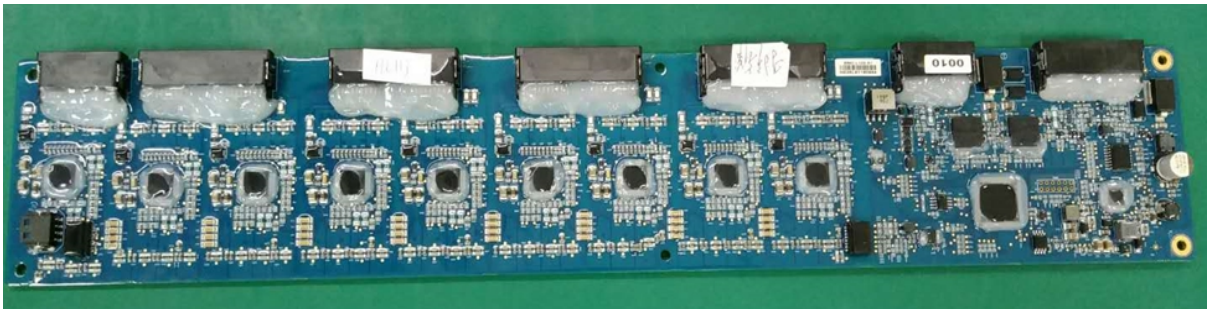
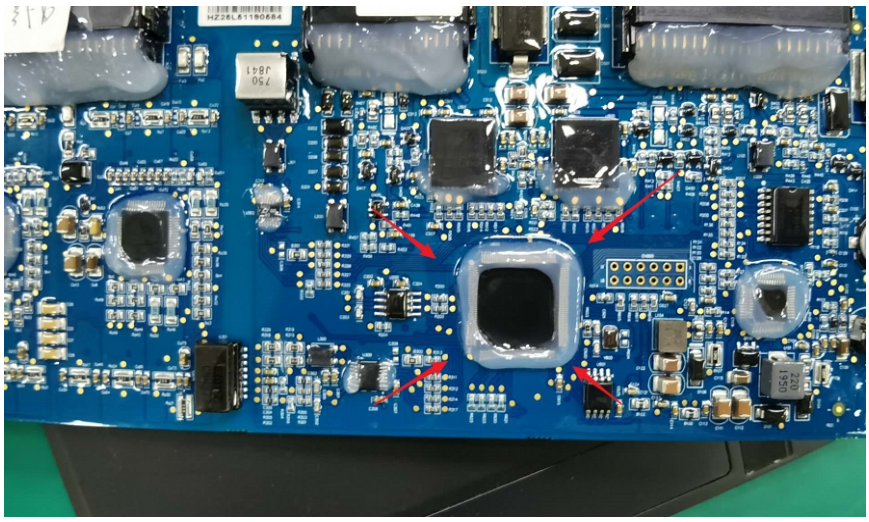


图 1 测试样件

图 2 测试过程

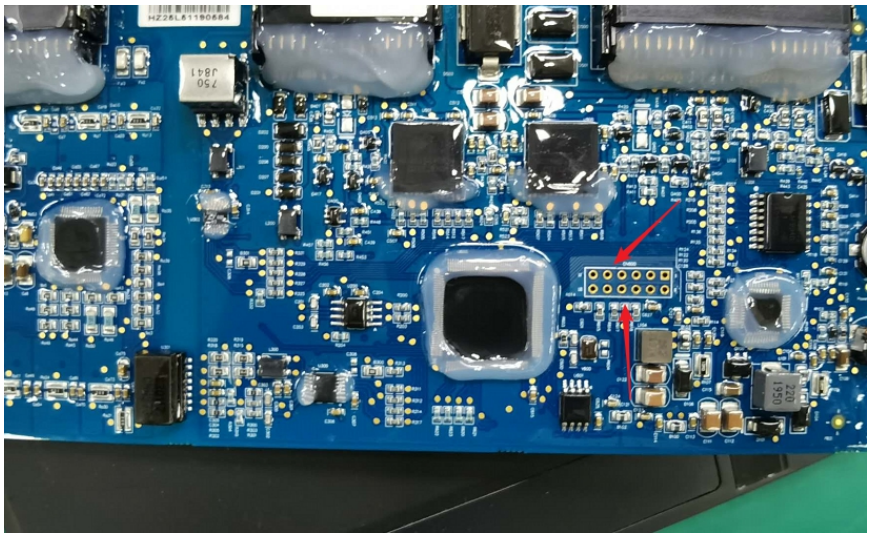
1）. 硬件安全测试 01(芯片封装)

测试编号	6.1a)1)
检测项	硬件安全测试（芯片封装）
符合性	符合☐　　不符合☑
测试评价方法	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
检测过程	BYD 提供了芯片型号：TC234，公网下载 tc234-data-datasheet，硬件工

	程师通过观察可以看出封装的方式为 TQFP-144；并且与供应商确认该封装方式
预期结果	车内充电系统关键芯片采用 BGA/LGA 等封装
检测结果	采用 TQFP-144 封装
截图	

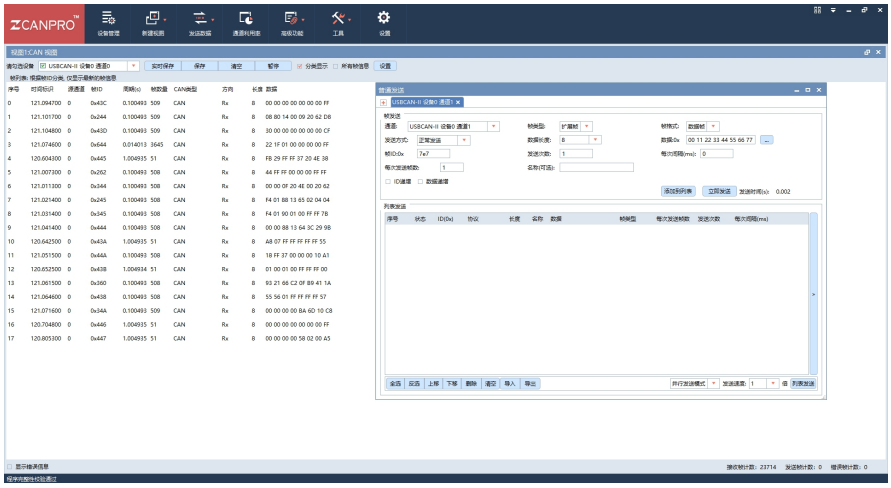
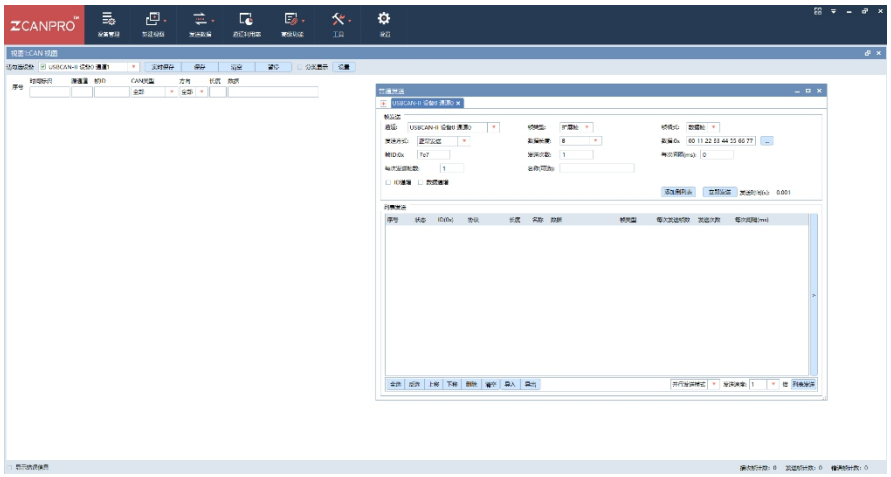
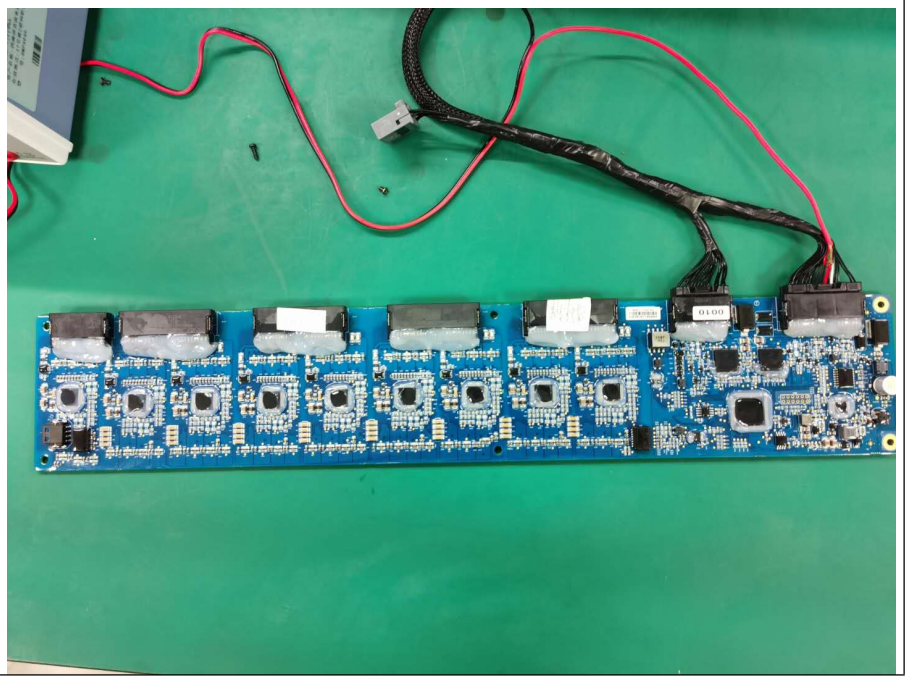
2）. 硬件安全测试 02（调试接口）

测试编号	6.1a)2)
检测项	硬件安全测试（调试接口）
符合性	符合☑　　不符合☐
测试评价方法	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。
检测过程	通过检查设计文档方法和与厂商沟通确定上市产品包含的调试接口，确定是否禁用了调试接口或进行安全访问控制；通过开盒观察或者使用专业的调试设备对产品进行调试，查看是否具有安全访问控制功能。
预期结果	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。
检测结果	存在调试 JTAG 接口,调试口的鉴权机制通过供应商提供报告说明。

截图	

3）. 硬件安全测试 03（总线隔离）

测试编号	6.1a)3)
检测项	硬件安全测试（总线隔离）
符合性	符合☑　　不符合☐
测试评价方法	查看测试样件（BMS 控制器）的直流充电通信 CAN 接口和车内 CAN 接口是否存在物理隔离，查看连接通信网络的节点是否只有非车载充电机和 BMS 两个控制器。
预期结果	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。
检测过程	通过检查设计文档方法和与厂商沟通确定测试样件（BMS 控制器）的直流充电通信 CAN 接口和车内 CAN 接口。检查测试样件（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是否只有非车载充电机和 BMS 两个控制器，再无其他控制器。 CAN0 和 CAN1 相互发送数据，都没有接收到对方发送的数据。
检测结果	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。

截图	  

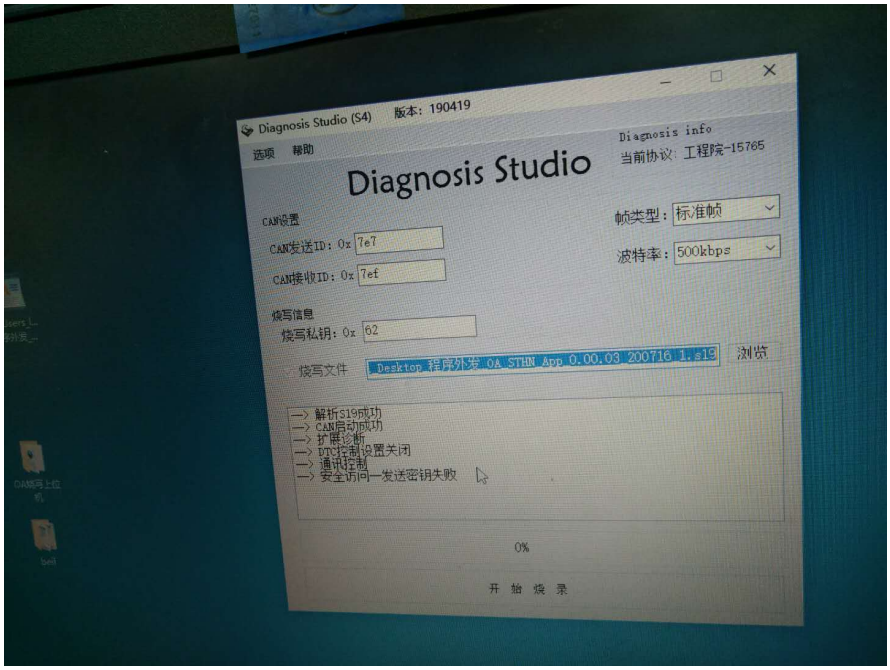
4）. 软件安全测试（安全启动）

测试编号	6. 2. 1a)
检测项	软件安全测试（安全启动）
符合性	符合☐　　不符合☐

测试评价方法	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。
测试过程	涉及知识产权，厂商不方便提供系统固件刷写包和刷写方式，未作测试。
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。
检测结果	未作测试。
截图	/

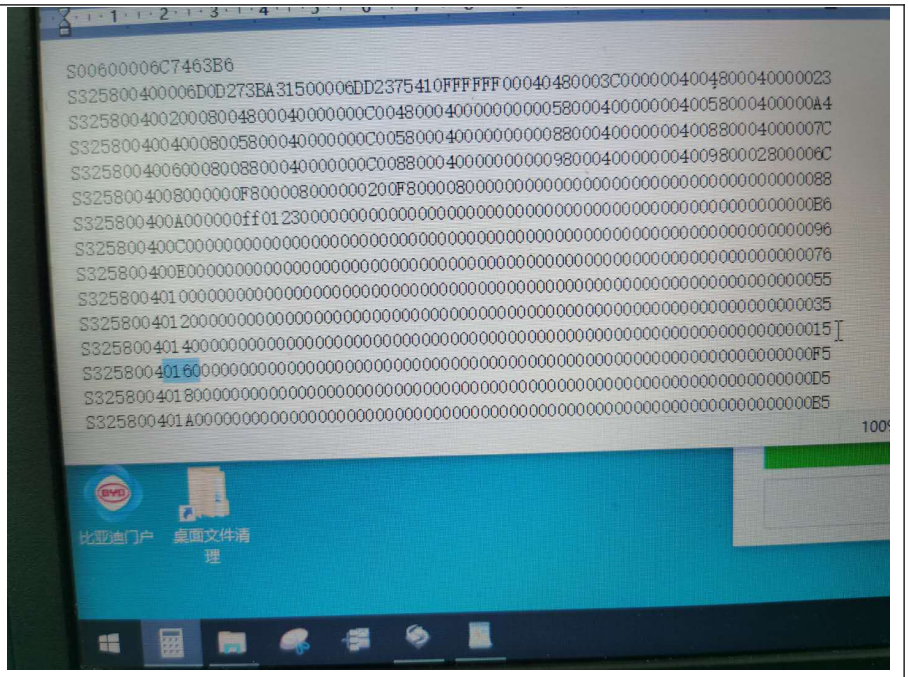
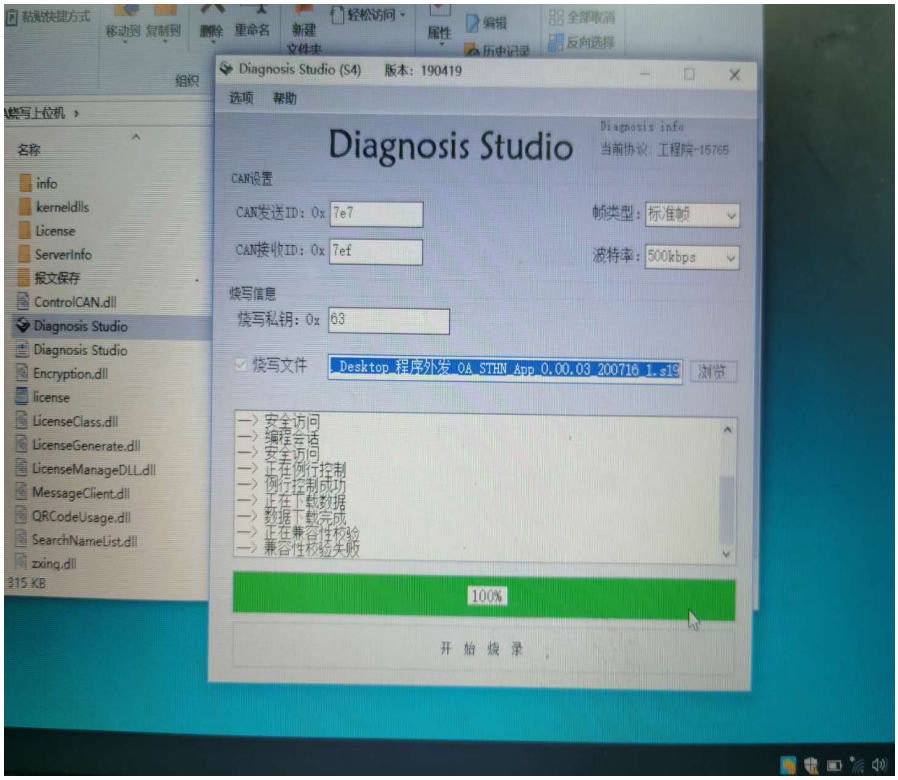
5）.软件安全测试 01（安全更新）

测试编号	6.2.2a)1)
检测项	软件安全测试 01（安全更新）
符合性	符合☑　　不符合☐
测试评价方法	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。
检测过程	1)　与厂商沟通，确定升级流程中的安全访问步骤（签名，加密等）； 2)　对其中的安全访问步骤进行破坏（更改签名，修改密钥（63 改成 62）等），查看升级安全步骤是否通过。
预期结果	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。
检测结果	修改更新密钥后无法更新。

截图	

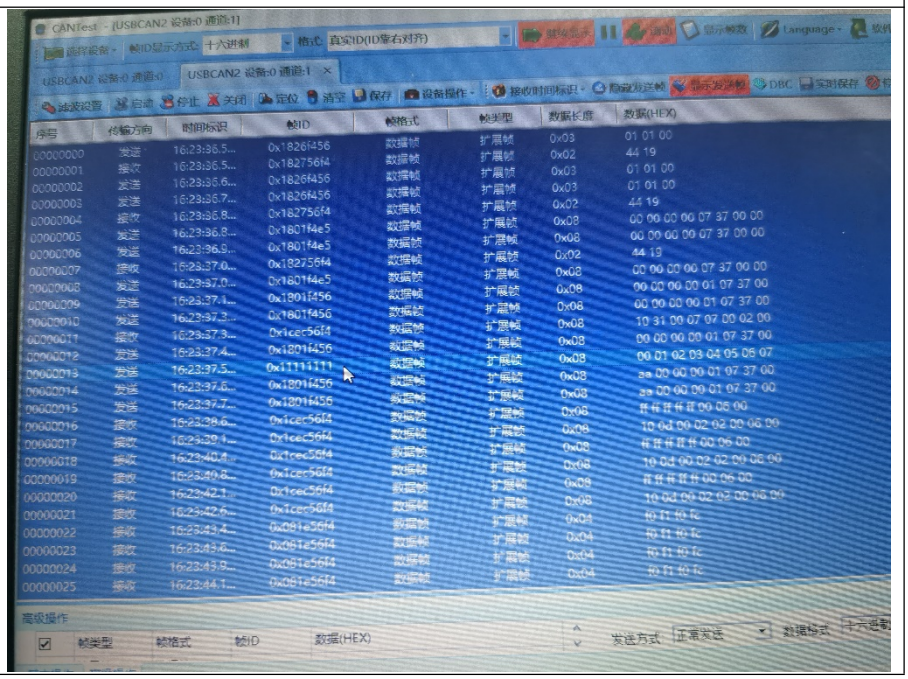
6）. 软件安全测试 02（安全更新）

测试编号	6.2.2a)2)
检测项	软件安全测试 02（安全更新）
符合性	符合☐　　不符合☑
测试评价方法	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。
检测过程	1）　与厂商沟通，获取正确的升级程序文件（s19）；并使用二进制编辑工具对文件进行修改，修改了一部分数据字段的值（0123）； 2）　检查程序是否对升级包进行了数据完整性验证，是否可完成车内充电系统软件更新。
预期结果	升级过程中对升级程序文件进行了完整性验证，无法更新车内充电系统软件。
检测结果	修改了一部分数据字段的值，可以更新成功。

截图	 

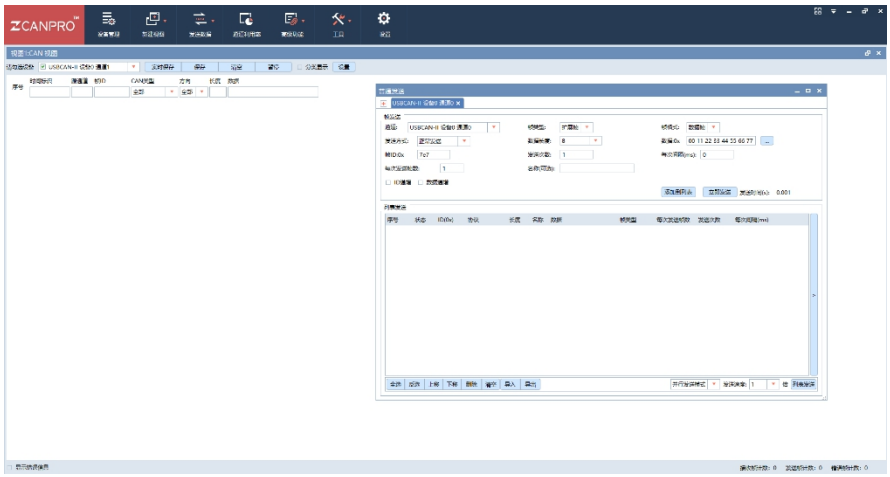
7）. 通信安全测试 01（通信接口）

测试编号	6.4.1.3a)1)
检测项	通信安全测试 01（通信接口）
符合性	符合☐　不符合☑
测试评价方法	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，检查通信是否会中断。
检测过程	模拟充电过程中直流 CAN 的收发消息，并在期间插入一条非充电数据。
预期结果	车内充电系统在接收到非充电系统协议或非主机厂规定协议时通信会中断，无法继续充电流程。
检测结果	充电过程未中断。
截图	

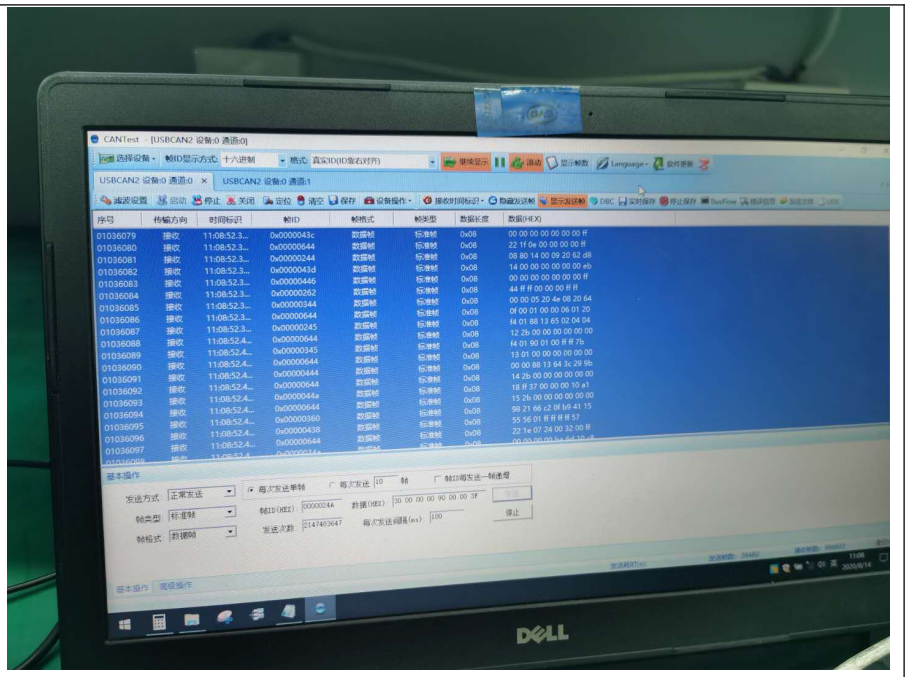
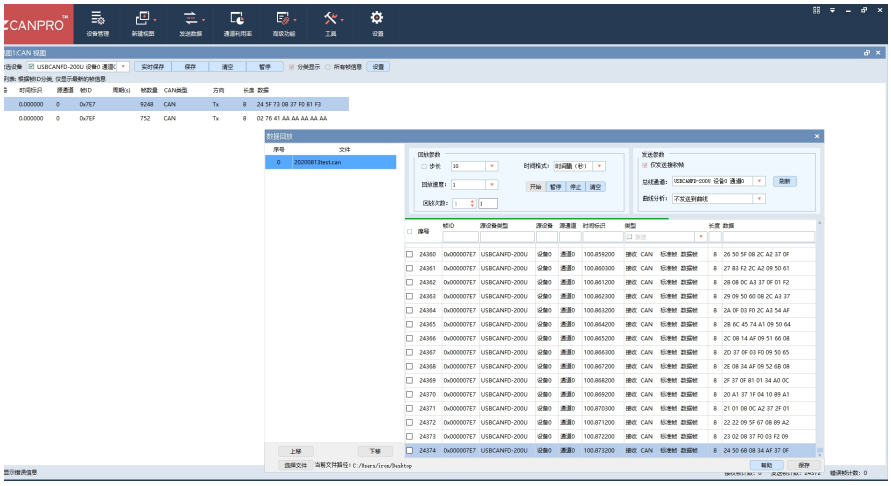
8）. 通信安全测试 02（通信接口）

测试编号	6.4.1.3a)2)
检测项	通信安全测试 02（通信接口）
符合性	符合☑　不符合☐
测试评价方法	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。
检测过程	尝试能否从直流 CAN 接收到车身 CAN 的数据。
预期结果	无法获取到任何车内通信数据。
检测结果	无法访问车内通信数据。

截图	

9）. 通信安全测试 03（通信接口）

测试编号	6.4.1.3a)3)
检测项	通信安全测试 03（通信接口）
符合性	符合☑　　不符合☐
测试评价方法	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。
检测过程	设备接入直流充电通信 CAN 接口，向车内充电系统发送诊断，刷写和标定样例数据（先尝试获取，如无法获取则厂商提供，例如系统刷写的数据）；查看车内充电系统是否有响应。
预期结果	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。
检测结果	通过直流充电通信 CAN 接口进行诊断等操作，车内无响应。

截图	 

3. 试验验证总结与分析

测试结果汇总如表2。

表2 测试结果汇总

序号	测试编号	测试名称	标准要求	测试结果	符合性
1	6.1a)1)	硬件安全测试（芯片封装）	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	采用TQFP-144封装	不符合
2	6.1a)2)	硬件安全测试（调试接口）	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	存在调试JTAG接口,调试口的鉴权机制通过供应商提供报告说明	符合

3	6.1a)3)	硬件安全测试（总线隔离）	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,查看连接通信网络的节点是否只有非车载充电机和BMS两个控制器	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	符合
4	6.2.1a)	软件安全测试01(安全启动）	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	厂商不方便提供刷写包,未作测试	无结果
5	6.2.2a)1)	软件安全测试02(安全更新）	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	修改更新密钥后无法更新	符合
6	6.2.2a)2)	软件安全测试03(安全更新）	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	修改了一部分数据字段的值，可以更新成功	不符合
7	6.4.1.3a)1)	通信安全测试01(通信接口）	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，检查通信是否会中断	充电过程未中断	不符合
8	6.4.1.3a)2)	通信安全测试02(通信接口）	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	无法访问车内通信数据	符合
9	6.4.1.3a)3)	通信安全测试03(通信接口）	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	通过直流充电通信CAN接口进行诊断等操作，车内无响应	符合

表3 测试覆盖标准条款

序号	项目	数量	备注
1	总测试项	21（100%）	详细测试小项
2	已测试	9（43%）	符合（5）；不符合（3）；无结果（1）
3	未测试	12（57%）	产品功能不支持（12）

本标准的测试验证项目总计21项，实际执行测试验证项目9项，未执行测试验证项目12项，通过测试项目5项。通过验证结果分析结论如下：

1.试验验证标准条款中，6.1a)1)未能通过，技术要求是“宜”，非强制要求； 6.2.2a)2)未能通过，考虑到要求过高，改为“宜”； 6.4.1.3a)1)未能通过，根据目前设计情况，将“检查通信是否会中断”改为“检查车内充电系统是否会响应”会更加合理；6.2.1a)未进行测试，供应商不方便提供系统固件刷写包和刷写方式，因涉及知识产权，需要测试部门研究新的测试方法。

2.因本标准全部条款适用于即插即充、无线充电场景，且部分技术条款具有前瞻性，实现即插即充、无线充电功能的产品较少，目前未能征集到相关产品，所以未能验证全部标准条款，试验验证标准条款覆盖率达43%，目前，还在在征集涵盖全条款功能的试验样件。

四、明确标准中涉及专利的情况

本标准不涉及专利问题。

五、预期达到的社会效益等情况

本标准的制定和实施，将为行业管理部门提供技术支撑，引导汽车充电系统产品满足行业对电动汽车充电系统信息安全的需求，推动电动汽车充电系统在车辆上的安全应用，大大提升我国车辆安全技术水平。

随着汽车电动化、智能化、网联化的发展，智能充电（如即插即充、无线充电）成为发展趋势。新功能的增加会带来很多信息安全问题，新技术标准项目实施有利于促进电动汽车在充电系统方面信息安全技术的发展，是引导产业创新发展的关键核心技术标准项目，具有显著的经济效益和社会效益。

六、采用国际标准和国外先进标准的情况

本标准没有采用国际标准。

本标准制定过程中未查到同类国际、国外标准。

七、与现行相关法律、法规、规章及相关标准的协调性

本标准与我国现行有关法律、法规和强制性国家标准不矛盾。

八、重大分歧意见的处理经过和依据

无。

九、标准性质的建议说明

根据标准化法和有关规定，建议本标准的性质为推荐性国家标准。

十、贯彻标准的要求和措施建议

1.首先应在实施前保证本标准文本的充足供应，使每个制造厂、设计单位以及检测机构等都能及时获得本标准文本，这是保证新标准贯彻实施的基础。

2.本次制定的《电动汽车充电系统信息安全技术要求》不仅与生产企业有关，而且与设计单位、检测机构等相关。对于标准使用过程中容易出现的疑问，起草单位有义务进行必要的解释。

3.可以针对标准使用的不同对象，如制造厂、质量监管等相关部门，有侧重点地进行标准的培训和宣贯，以保证标准的贯彻实施。

4.建议本标准批准发布6个月后实施。

十一、废止现行相关标准的建议

无。

十二、其他应予说明的事项

无。