ICS 43.080
CCS T43

T/HEVCA

海南省电动汽车与充电设施协会团体标准

T/HEVCA 1.9—2023

换电式纯电动重型载货汽车及共享换电站建设通用技术要求 第9部分：通讯及数据安全管理要求

General technical requirements for battery swap electric heavy goods vehicles and shared battery swap station
Part 9:Communnication and data security management requirements

2023－12－26 发布　　2024－1－1 实施

海南省电动汽车与充电设施协会　　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。

本文件是T/HEVCA 1《换电式纯电动重型载货汽车及共享换电站建设通用技术要求》的第9部分。T/HEVCA 1已经发布了以下部分：

——第1部分：总则；
——第2部分：换电电池系统通用技术要求；
——第3部分：换电底托通用技术要求；
——第4部分：换电连接器通用技术要求；
——第5部分：换电控制器通用技术要求；
——第6部分：换电系统通讯协议技术要求；
——第7部分：换电系统设备通用技术要求；
——第8部分：共享换电站建设及验收技术要求；
——第9部分：通讯及数据安全管理要求。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由海南省新能源汽车促进中心提出。

本文件由海南省电动汽车与充电设施协会归口。

本文件起草单位：海南省新能源汽车促进中心、海南省电动汽车与充电设施协会、上海启源芯动力科技有限公司、上海玖行能源科技有限公司、上海融青新能源科技有限公司、中油绿色能源（海南）有限公司、海南省充电产业投资公司、南方电网（海南）电动汽车服务有限公司、海南省充换电一张网服务有限责任公司、南方电网数字电网集团（海南）有限公司、海南电力产业发展有限责任公司、绿动未来投资集团（海南）有限公司、万帮数字能源股份有限公司、海南奥动新能源科技有限公司、上海融和智电新能源有限公司、东风柳州汽车有限公司、汉马科技集团股份有限公司、徐州徐工新能源汽车有限公司、海南远程新能源载货汽车有限公司、海南山益工程机械有限公司、江苏智慧优视电子科技有限公司、国机海南发展有限公司、海南促进新能源汽车科技有限公司。

本文件主要起草人：钟东、何瑞辉、罗浩亮、郭国柱、雒宏武、陈礼丽、周文杰、张彬、冯志鹏、黎茹、凌凯、何文卫、林尤超、陈淮、张熙远、何滨华、金凯、孙俊伟、李士汉、黎传冠、李伟宁、林杰、赵亮、陈光、王运豪、陶涛、王玉超、陈德、玄先涛、赵银山、吉春宇、何雪海、吴清岩、许林勇、曾伟、刘英山、曹拥华、范志勇、刘子翔、万术伟、苏运荣、林芳弘。

引　言

在“双碳”目标指引下，载货汽车行业正加速向绿色低碳方向发展。其中，换电式纯电动重型载货汽车由于车电分离、快速补能的技术特点，受到行业高度关注。随着换电式纯电动重型载货汽车渗透率不断提高，市场上不同的换电站生产商越来越多，不同技术路径之间差异明显。

T/HEVCA 1旨在规范重型载货汽车换电机构的技术要求和试验方法，统一换电接口的界面型式与结构尺寸，确立换电站设备的技术要求和试验方法，指导换电站的建设与验收，确立数据监管平台的安全管理要求，从而实现不同换电站生产商与电动重型载货汽车生产商之间的产品互联互通，实现换电资源共享。T/HEVCA 1由九部分组成。

——第1部分：总则。目的在于确立换电式纯电动重型载货汽车及共享换电站的基本功能以及换电步骤，确保产品的功能性。

——第2部分：换电电池系统通用技术要求。目的在于确立换电电池系统的结构尺寸、技术要求及试验方法等，用于实现换电电池系统的互换性。

——第3部分：换电底托通用技术要求。目的在于确立换电底托的结构尺寸以及技术要求等，用于实现换电底托的互换性。

——第4部分：换电连接器通用技术要求。目的在于确立换电连接器的结构尺寸、电气接口定义、技术要求以及试验方法等，用于实现换电连接器的兼容性和互换性。

——第5部分：换电控制器通用技术要求。目的在于确立换电控制器的功能要求、性能要求、通讯要求、技术要求以及试验方法等，用于实现换电控制器的兼容性和互换性。

——第6部分：换电系统通讯协议技术要求。目的在于确立换电系统的通讯协议，用于实现换电系统的兼容性和互换性。

——第7部分：换电系统设备通用技术要求。目的在于确立换电系统设备的技术要求以及试验方法等，用于实现换电系统设备的互换性。

——第8部分：共享换电站建设及验收技术要求。目的在于确立换电站的选址、规划、系统、安全与消防要求等，用于指导共享换电站的建设及验收。

——第9部分：通讯及数据安全管理要求。目的在于确立共享换电站与政府监管平台的数据采集与监管要求，用于实现换电数据的统一管理。

换电式纯电动重型载货汽车及共享换电站建设通用技术要求 第9部分：通信及数据安全管理提要求

1 范围

本文件规定了换电式纯电动重型载货汽车共享换电站与管理平台的换电服务数据采集与监管要求、数据安全管理及风险预警的相关要求。

本文件适用于纯电动载货汽车吊装式换电站。不适用于侧换式及底部换电式。

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。

GB/T 22239 信息安全技术网络安全等级保护基本要求

GB/T 22240 信息安全技术网络安全等级保护定级指南

GB/T 27930 非车载传导式充电机与电动汽车之间的数字通信协议

GB/T 29317-2021 电动汽车充换电设施术语

GB/T 32960.3 电动汽车远程服务与管理系统技术规范 第3部分：通讯协议与格式

NB/T 33005 电动汽车充电站及电池更换站监控系统技术规范

T/CEC 102.1-2021 电动汽车充换电服务信息交换

T/CEC 102.2-2021 电动汽车充换电服务信息交换 第2部分：公共信息交换规范

T/CEC 102.3-2021 电动汽车充换电服务信息交换 第3部分：业务信息交换规范

T/CEC 102.4-2021 电动汽车充换电服务信息交换 第4部分：数据传输与安全

T/HEVCA 1.5-2023 换电式纯电动重型载货汽车及共享换电站建设通用技术要求 第5部分：换电控制器通用技术要求

T/HEVCA 1.6-2023 换电式纯电动重型载货汽车及共享换电站建设通用技术要求 第6部分：换电系统通讯协议技术要求

3 术语和定义

GB/T 29317-2021、GB/T 29772界定的术语和定义适用于本文件

4 换电服务数据采集与监管要求

4.1 换电服务体系通信架构

下列系统参与换电服务信息交换，架构如图1所示：

a) 换电电池系统；

b) 换电控制器；

c) 站控系统；

d) 运营服务平台；

e) 一张网平台及海南省新能源汽车监管平台/一张网平台。

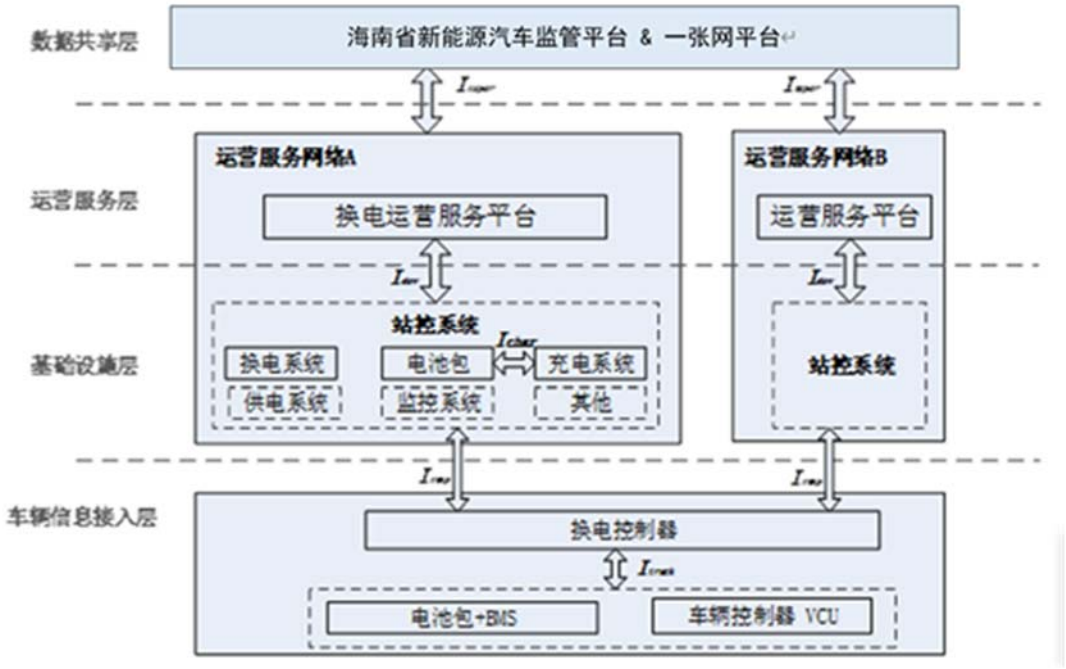

图 1 纯电动载货汽车换电服务体系参与实体与通信架构

4.2 换电控制器要求

4.2.1 换电控制器与电池系统的信息交互应满足 GB/T 32960.3 的相关要求。

4.2.2 换电控制器与站控系统之间的数据交互，应满足 T/HEVCA 1.5-2023 中 5.4.3 的相关要求。

4.3 站控系统要求

4.3.1 一般要求

4.3.1.1 站控系统应具备下列功能：

a) 站内设备监视；
b) 设备状态报警；
c) 站内设备控制与操作；
d) 事件记录。

4.3.1.2 站控系统应具备下列单元：

a) 站内充电监控单元；
b) 电池系统更换监控单元。

4.3.1.3 站控系统宜具备下列单元：

a) 供电监控单元；
b) 视频及环境监控单元；
c) 网络及通信接口单元。

4.3.1.4 站控系统的数据采集的间隔时间应不大于 1 s。

4.3.1.5 站控系统与运营管理平台交互数据应包括下列信息：

a) 车辆认证信息；
b) 站点实时信息；
c) 换电过程信息；
d) 换电记录；

e） 充电记录；
f） 补发信息；
g） 告警信息；
h） 配置信息；
i） 控制信息。

4.3.1.6 站控系统应具备本地保存及断点续传功能。本地保存的补发信息，数据保存时长应不低于24小时。

4.3.2 站内充电监控单元

4.3.2.1 站内充电监控单元应满足NB/T 33005附录B的相关要求，并应采集及存储下列数据：
a） 电池系统类型；
b） 电池系统电压；
c） 充电机直流输出电流；
d） 充电机温度；
e） 充电机状态；
f） 电池系统充电时间；
g） 电池系统充电电能；
h） 单体蓄电池电压；
i） 单体蓄电池荷电；
j） 电池系统温度；
k） 电池系统故障代码信息。

4.3.2.2 充电机与电池系统的信息交互应满足GB/T 27930的相关要求，宜存储下列信息：
a） 电池系统电流请求信息；
b） 绝缘状态信息；
c） 电池系统温度；
d） 电池系统故障代码；
e） 采集时间；
f） 充电机交流侧开关状态；
g） 充电机直流侧开关跳闸/熔断器熔断状态；
h） 监控单元故障；
i） 充电架编号及空置/就位状态；
j） 电池系统温度。

4.3.3 电池更换监控单元

4.3.3.1 电池更换监控单元的数据采集与存储应满足NB/T 33005附录B的相关要求。

4.3.3.2 站控系统应向运营管理平台实时发送下列信息：
a） 换电系统启动信息；
b） 工作及停止的状态量信息；
c） 换电完成信息。

4.3.3.3 电池更换监控单元应可接受运营管理平台的远程控制。

4.3.4 供电监控单元

供电监控单元的数据采集与存储应满足NB/T 33005附录B的相关要求。

4.4 运营管理平台要求

4.4.1 一般要求

4.4.1.1 运营管理平台应具备下列功能：

a) 站点监控；
b) 站点管理；
c) 电池管理；
d) 车辆管理。

4.4.1.2 运营管理平台宜具备下列功能：
a) 收费账务；
b) 清分结算；
c) 资产管理；
d) 综合统计分析；
e) 系统管理。

4.4.1.3 运营管理平台应建立数据库，具备实时数据和历史数据查询功能。

4.4.1.4 站控系统与运营管理平台之间的数据交互，宜满足 T/CEC 102.1-2021 的相关要求。

4.4.2 数据采集要求

4.4.2.1 运营管理平台接收站控系统转发的数据，数据应包括电池类数据与换电站数据。

4.4.2.2 电池类数据应包括下列信息：
a) 数据采集时间；
b) 电池包电压；
c) 工作电流；
d) SOC 剩余量；
e) 充电次数；
f) 换电次数；
g) 电池累计运行里程；
h) 电池充电总容量；
i) 电池充电总能量；
j) 电池换电站内充电总容量；
k) 电池换电站内充电总能量；
l) 电池输出总容量；
m) 电池输出总能量；
n) 站内输出总容量；
o) 站内输出总能量。

4.4.2.3 电池类数据宜包括下列信息：
a) 电池单体电压；
b) 单体温度；
c) 最高温度；
d) 最高电压；
e) 故障信息。

4.4.2.4 换电站数据应包括下列信息：
a) 换电站运行状态数据；
b) 整站相关子系统运行状态数据；
c) 车辆信息数据；
d) 换电站配置数据。

4.5 一张网平台通信要求

运营管理平台与一张网平台的数据交互应满足T/CEC 102.1-2021、T/CEC 102.2-2021、T/CEC 102.3-2021、T/CEC 102.4-2021的相关要求。

4.6 电池包及 BMS 与车辆控制器通信要求

采用CAN通信方式的电池系统BMS与车辆控制器（VCU）在换电站内与其相连接的设备之间的通讯方式应满足T/HEVCA 1.6-2023的相关要求。

4.7 数据质量

4.7.1 主要技术要求除充电机充电启动过程之外的数据上传周期应在30秒以内。

4.7.2 数据可靠性应满足下列要求：

a) 模拟量测量综合误差≤1 %；
b) 系统可用率≥99.9 %；
c) 遥测合格率≥98 %；
d) 遥控正确率≥99.99 %；
e) 遥信正确率≥99 %；
f) 站控层平均故障间隔时间（MTBF）≥5000 h；
g) 功能层平均故障间隔时间（MTBF）≥5000 h。

4.7.3 数据系统实时性应满足下列要求：

a) 模拟量越死区传送时间（至站控层显示屏）≤2 s；
b) 开关量变位传送时间（至站控层显示屏）≤1 s；
c) 开关量信号输至画面显示响应时间≤2 s；
d) 系统控制操作响应时间（从发出指令到现场变位信号返回）≤4 s
e) 实时数据扫描周期≤2 s；
f) 画面实时数据更新周期≤3 s；
g) 动态画面响应时间≥2 s。

5 数据安全管理

5.1 基本要求

5.1.1 应根据平台系统的重要程度以及遭到破坏后的危害程度，按照GB/T 22240的要求，确定其安全保护等级，并具备GB/T 22239规定的基本安全保护能力。

5.1.2 应根据平台系统的应用、数据及技术架构，将系统信息进行分等级管理。并应根据其重要程度划分安全信息区域，采取不同的系统安全保护措施，实现同等级信息集中管理。

5.2 完整性要求

5.2.1 应确保采取的数据信息管理和技术措施以及覆盖范围的完整性。

5.2.2 应能够检测网络设备操作系统、主机操作系统、数据库管理系统和应用系统的系统管理数据。

5.2.3 当信息和重要业务数据的完整性在存储过程中受到破坏时，应采取必要的恢复措施。

5.2.4 应具备完整的用户访问、处理、删除数据信息的操作记录能力。

5.2.5 在传输数据信息时，经过不安全网络的，应对传输的数据提供完整性校验。

5.3 保密性与真实性要求

5.3.1 应采用有效的加密措施，实现重要业务数据信息传输及存储保密性。

5.3.2 宜采用区块链技术保障重要业务数据信息真实可信。

5.4 数据信息备份与恢复

5.4.1 数据信息备份应采用性能可靠、不易损坏的介质，如光盘、硬盘等。

5.4.2 备份数据信息的物理介质应注明数据信息的来源、备份日期、恢复步骤等信息，并置于安全环境保管。

5.4.3 系统应提供重要数据的本地数据备份或者云端数据定期备份功能，防止未经授权的备份数据访问。

5.4.4 系统应具备故障后数据恢复功能，应能实现本地数据和云端数据的同步。

5.4.5　运维操作员应根据不同业务系统实际拟定需要测试的备份数据信息以及测试的周期。
5.4.6　本地数据和云数据操作时需要具备相应权限，不同权限的人员只能对数据执行授权范围内的数据操作。
5.4.7　对于因设备故障、操作失误等造成的一般故障，需要恢复部分设备上的备份数据信息，遵循异常事件处理流程，由运维操作员负责恢复。
5.4.8　应尽可能地定期检查和测试备份介质和备份信息，保持其可用性和完整性，并确保在规定的时间内恢复系统。
5.4.9　应确定重要业务信息的保存期以及其它需要永久保存的归档拷贝的保存期；恢复程序应定期接受检查及测试，以确保在恢复操作程序所预定的时间内完成。

5.5　应用安全

5.5.1　运营管理平台应部署应用防火墙、入侵检测、日志审计系统、数据库审计系统等措施进行安全防护。
5.5.2　运营管理平台应具备权限控制能力。

6　风险预警

6.1　资源使用预警

6.1.1　系统应实时监控云平台及站端服务器及数据库，应至少监控包括下列数据：
a)　CPU 使用率；
b)　内存使用率；
c)　磁盘空间使用率；
d)　网络带宽使用情况。
6.1.2　系统应设定合理的预警阈值，当实际使用高于预警阈值时，应能触发风险预警，由运维操作人员及时处理。

6.2　平台服务及数据库性能预警

6.2.1　系统应实时监控云平台主要服务及数据库性能指标，应至少监控下列指标：
a)　服务响应时间；
b)　查询速度；
c)　事务处理速度。
6.2.2　系统应设定合理的预警阈值。当实际性能指标与预警阈值对比出现异常时，应能触发风险预警，由运维操作人员及时处理。