ICS 29.200
CCS K81

T/IMAS

团 体 标 准

T/IMAS 052.7—2022

电动中重卡共享换电站及车辆换电系统技术规范 第七部分：数据安全管理，风险预警分析技术要求

Electric medium and heavy truck sharing battery swap station and technical specification of battery swap system
Part7:Technical requirement of data security management and risk warning analysis

2022－12－01 发布 2022－12－02 实施

内蒙古标准化协会 发 布

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T/IMAS 052—2022《电动中重卡共享换电站及车辆换电系统技术规范》分为8个部分：

——第一部分：总则；

——第二部分：换电车辆换电电池箱体与换电底托技术要求；

——第三部分：换电车辆换电连接器技术要求；

——第四部分：换电车辆换电控制器技术要求；

——第五部分：换电系统设备技术安全；

——第六部分：换电系统通讯协议技术要求；

——第七部分：数据安全管理，风险预警分析技术要求；

——第八部分：换电站的规划布局及安装防护要求。

本文件为T/IMAS 052.7—2022《电动中重卡共享换电站及车辆换电系统技术规范》的第七部分。

本文件由北奔重型汽车集团有限公司提出。

本文件由内蒙古标准化协会归口。

本文件起草单位：北奔重型汽车集团有限公司、上海启源芯动力科技有限公司、协鑫能源科技有限公司、上海玖行能源科技有限公司、宁德时代新能源科技股份有限公司。

本文件主要起草人：于文明、白晓龙、袁胜东、栓柱、温金雄、王松旺、彭涛、来瑞俊、刘丽芳、赵杰、王伟光。

电动中重卡共享换电站及车辆换电系统
技术规范
第七部分：数据安全管理，风险预警分析技术要求

1 范围

本标准规定了电动中重卡换电站的数据安全管理，风险预警分析等技术要求。

本标准适用于电动中重型卡车换电站。

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

NB/T 33005-2013 电动汽车充电站及电池更换站监控系统技术规范

NB/T 33017-2015 电动汽车智能充换电服务网络运营监控系统技术规范

3 术语和定义

本文件没有需要界定的术语和定义。

4 数据上传要求、数据质量评估

4.1 监控系统

4.1.1 建设原则

有利于实现全系统的信号采集、安全稳定控制和事故/故障处理，提供系统运行的可靠性、经济性，确保充电及电池更换的安全性。系统宜采用数字化、网络化、智能化、集成化的先进高效技术，简化硬件配置，避免重复，实现资源共享。

4.1.2 系统构成

监控系统宜由换电管理平台、站控层、功能层三部分组成，并用分层、分布、开放式网络实现连接。

换电管理平台宜采用分区分层架构，满足总部、运营商、站级三级应用。

站控层由计算机网络连接的主机/操作员工作站和各种功能站构成，提供站内运行的人机界面，实现控制、管理功能层设备等功能，形成全站的监控、管理中心，并具备与换电管理平台通信的功能。

功能层由站内充电监控单元、电池更换监控单元、供电监控单元、视频及环境监控单元、各种网络、通信接口设备等构成，其中充电监控单元和电池更换监控单元为标配设备，其他为选配设备，可根据换电站功能配置选配。

4.1.3 系统功能

换电管理平台宜具备收费账务、清分结算、资产管理、综合统计分析及系统管理等功能。

换电管理平台应建立数据库，可进行实时数据和历史数据查询，且便于数据统计、汇总、分析。

换电管理平台应具有站点监控、站点管理、电池管理、车辆管理等功能。

站控系统应具备站内设备监视、设备状态报警、站内设备控制与操作、事件记录等功能。

站控系统应建立数据库，具备人机交互界面、统计计算等功能。

功能层应具备充电监控、电池更换监控、视频及环境监控等功能。

4.1.4 站控系统与上级平台通信协议结构优选 json 和 mqtt 协议

服务端平台对接收到的数据进行校验，当校验正确时，服务端平台做正确应答。当校验错误时，服务端平台做错误应答。服务端平台的应答信息错误时，客户端应重发本条实时信息。

平台交换数据和用户自定义数据存在时，完成平台交换数据和用户自定义数据的上报。向服务端平台上报信息的时间周期应可调整。

当终端发送数据为加密状态时，客户端平台应先进行数据解密，并重新加密后发送至服务端平台，如平台间传输无加密需求则无需重新加密。

补发机制：当数据通信链路异常时，客户端平台应将实时上报数据进行本地存储。在数据通信链路恢复正常后，在发送实时上报数据的空闲时间完成补发存储的上报数据。

数据包结构：一个完整的数据包应由报文主题、站点编码、数据加密方式、时间戳、消息体、数据签名组成。

4.1.5 指标要求

按照NB/T 33017-2015第10章、NB/T 33005-2013第7章部分。

a) 换电管理平台响应速度；
b) 系统容量、并发量；
c) 系统实时性指标；
d) 连续运行要求；
e) 年可用率；
f) 接收终端数据的成功率。

4.1.6 换电站路由服务

统一接收站控系统的硬件设备数据，通过mqtt协议实时转发至监控系统。

4.2 站控系统数据要求

4.2.1 通用规范

区分上传与下载数据。

区分本地保存和云端交互数据。

站控主机与云端交互数据应分为上传数据和下载数据，上传数据包括车辆认证信息、站点实时信息、换电过程信息、换电记录、充电记录、补发信息和告警信息，下载数据包括配置信息和控制。

本地保存的补发信息，数据保存时长至少不应低于24小时。数据采集的间隔时间宜不大于1 s。

4.2.2 电池箱数据

按照 NB/T 33005-2013附录B,应包含：电池箱电压、电池箱充电电流、电池箱充电功率、电池箱充电时间、电池箱充电电能、单体蓄电池电压、单体蓄电池荷电、电池箱温度、电池箱标识、电池箱类型、电池箱参数、电池箱故障代码等信息。

应包含绝缘电阻、绝缘等故障信息、故障前后实时信息以用于故障分析。宜包含功率、电流请求信息、充放电状态、车辆运行状态、GPS等实时信息（10 s）、数据产生时间。

应具有数据续传功能。

4.2.3 充电设备数据

按照NB/T 33005-2013附录B,应包含充电机直流输出电压、充电机直流输出电流、充电机温度、充电机状态、充电机故障代码等信息。

宜包含充电机交流侧开关状态、充电机直流侧开关跳闸/熔断器熔断、监控单元故障、监控单元与站内监控系统通信中断、充电架空置/就位状态、充电架充电进行/充电完成状态等信息。

4.2.4 换电站换电系统数据

按照NB/T 33005-2013附录B,应包含换电过程数据/信号，如：启动/停止/工作状态。

应具有远程控制功能。

4.2.5 供电设备数据

按照NB/T 33005-2013附录B,应包含：功率、电压、电流、温度等工作状态。

4.3 监控上级平台系统数据要求

4.3.1 通用规范

区分上传与下载数据。

区分本地保存和云端交互数据。

站控主机与云端交互数据应分为上传数据和下载数据,上传数据包括车辆认证信息、站点实时信息、换电过程信息、换电记录、充电记录、补发信息和告警信息，下载数据包括配置信息和控制。

部分数据需要进行本地保存，本地保存数据包括补发信息，数据采集周期不应超过30分钟，数据保存周期不应超过1小时。

数据采集的间隔时间应不大于1 s。

云端在相关定义和要求下，可通过远程对站控主机下达控制命令。

4.3.2 电池类数据

按照NB/T 33005-2013附录B,应包括电池包电压、工作电流、SOC、剩余容量、充电次数、换电次数、电池累计运行里程、电池充电总容量、电池充电总能量、电池换电站内充电总容量、电池换电站内充电总能量、电池输出总容量、电池输出总能量、站内输出总容量、站内输出总能量。

宜包括电池单体电压、单体温度、最高温度、最高电压、故障信息等。

应包含数据实际产生时间。

4.3.3 换电站数据

上传信息包括换电站运行状态数据、车辆信息数据、整站相关子系统运行状态数据。

下载信息包括：换电站配置数据、换电站远程操作数据等。

4.4 数据质量

4.4.1 主要技术指标

数据上传周期应在30秒以内。

4.4.2 可靠性指标

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。

4.4.3 系统实时性指标

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 换电站与服务平台通信

站控系统与云平台的通信协议结构宜按照《T/CEC 102-2016 电动汽车充换电服务信息交换》的规定，采用其中的通讯定义。

换电站与云平台的通讯应采用VPN或云专线等方式，实现点对点安全通信。

6 数据安全管理

6.1 基本要求

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的规定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。应根据平台系统的应用、数据和技术架构，将系统信息进行分等级管理，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。

6.2 数据信息完整性

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。

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、鉴别信息和重要业务数据在存储过程中完整性受到破坏，并在检测到完整性受到破坏时采取必要的恢复措施。

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。

在传输数据信息时，经过不完全网络时，应对传输的数据提供完整性校验。

应具备完善的权限管理测试，支持权限最小化原则、合理授权。

6.3 数据信息保密性与真实性

数据信息保密性安全规范用于保障业务平台重要业务数据信息的安全传递与处理应用，确保数据信息能够被安全、方便、透明的使用。为此，业务平台应采用加密等安全措施开展数据信息保密性工作。

应采用加密有效措施实现重要业务数据信息传输保密性。

应采用加密实现重要业务数据信息存储保密性。

应采用区块链技术保障重要业务数据信息真实可信。

6.4 数据信息备份与恢复

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。

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。

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。

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。

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。

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。

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。

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。

6.5 应用安全

系统应按照国家信息安全技术网络安全等级保护三级防护要求，部署相应的应用防火墙、入侵检测、日志审计系统、数据库审计系统等安全防护平台进行安全防护。

系统应能对登录的用户进行身份标识和鉴别，只有在系统注册后合法用户才能接入（前半句GB/T 22239,7.1.4.1）。

系统应对登录的用户分配账户和权限。

7 风险预警

7.1 资源使用预警

系统应实时监控云平台及站端服务器及数据库各项资源使用情况，包括但不限于CPU使用率、内存使用率、磁盘空间使用率、网络带宽使用情况等，并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。

7.2 平台服务及数据库性能预警

系统应实时监控云平台主要服务及数据库性能指标，包括但不限于服务响应时间、查询速度、事务处理速度等，并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。