|  |  |
| --- | --- |
| ICS | 43.080.01 |
| CCS | |  | | --- | |  |   T 47 |

团体标准

T/CASMES XXXX—2024

基于智慧城市的新能源汽车充电平台管理系统技术要求

Technical requirements for management system of new energy vehicle charging platform based on smart city

2024 - XX - XX发布

2024 - XX - XX实施

中国中小企业协会  发布

目次

[前言 III](#_Toc182991832)

[1 范围 1](#_Toc182991833)

[2 规范性引用文件 1](#_Toc182991834)

[3 术语和定义 1](#_Toc182991835)

[4 系统组成 2](#_Toc182991846)

[4.1 云平台层 2](#_Toc182991847)

[4.2 网络通信层 2](#_Toc182991848)

[4.3 充电设施层 2](#_Toc182991849)

[4.4 用户交互层 2](#_Toc182991850)

[4.5 运营管理层 3](#_Toc182991851)

[4.6 安全防护层 3](#_Toc182991852)

[5 系统设计要求 3](#_Toc182991853)

[5.1 开放性 3](#_Toc182991854)

[5.2 模块化与可扩展性 3](#_Toc182991855)

[5.3 稳定性与可靠性 3](#_Toc182991856)

[5.4 安全性 3](#_Toc182991857)

[6 功能要求 3](#_Toc182991858)

[6.1 用户管理 3](#_Toc182991859)

[6.2 充电管理 3](#_Toc182991860)

[6.3 运维管理 3](#_Toc182991861)

[6.4 数据分析与优化 4](#_Toc182991862)

[6.5 第三方平台接入 4](#_Toc182991863)

[6.6 用户体验 4](#_Toc182991864)

[7 性能要求 4](#_Toc182991865)

[7.1 系统响应时间 4](#_Toc182991866)

[7.2 系统可用性 4](#_Toc182991867)

[7.3 系统吞吐量 4](#_Toc182991868)

[7.4 数据准确性 4](#_Toc182991869)

[7.5 系统安全性 4](#_Toc182991870)

[7.6 系统兼容性 4](#_Toc182991871)

[8 互联互通与兼容性要求 4](#_Toc182991872)

[8.1 互联互通要求 4](#_Toc182991873)

[8.2 兼容性要求 5](#_Toc182991874)

[9 信息安全 5](#_Toc182991875)

[9.1 系统平台安全 5](#_Toc182991876)

[9.2 数据存储安全 5](#_Toc182991877)

[10 实施与运维要求 5](#_Toc182991878)

[10.1 实施要求 5](#_Toc182991879)

[10.2 运维要求 5](#_Toc182991880)

1. 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。

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。

本文件由温州城市一卡通服务有限公司提出。

本文件由中国中小企业协会归口。

本文件起草单位：温州城市一卡通服务有限公司、

本文件主要起草人：

基于智慧城市的新能源汽车充电平台管理系统技术要求

* 1. 范围

本文件规定了基于智慧城市的新能源汽车充电平台管理系统的系统组成、系统设计要求、功能要求、性能要求、互联互通与兼容性要求、信息安全、实施与运维要求。

本文件适用于为新能源汽车用户提供充电服务的各类机构和组织等。

* 1. 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 20271 信息安全技术 信息系统通用安全技术要求

GB/T 20273 信息安全技术 数据库管理系统安全技术要求

GB/T 22239 信息安全技术 网络安全等级保护基本要求

GB/T 31168 信息安全技术 云计算服务安全能力要求

* 1. 术语和定义

下列术语和定义适用于本文件。



智慧城市 smart city

运用信息和通信技术手段感测、分析、整合城市运行核心系统的各项关键信息，对包括民生、环保、公共安全、城市服务、工商业活动在内的各种需求做出智能响应，实现城市智慧式管理和运行，进而为城市中的人创造更美好的生活，促进城市的和谐、可持续成长。



新能源汽车 new energy vehicles

指采用非常规的车用燃料作为动力来源（或使用常规的车用燃料、采用新型车载动力装置），综合车辆的动力控制和驱动方面形成的技术原理先进、具有新技术、新结构的汽车。新能源汽车包括纯电动汽车、增程式电动汽车、混合动力汽车、燃料电池电动汽车、氢发动机汽车等。



充电平台管理系统 charging platform management system

基于智慧城市架构，用于管理、监控和优化新能源汽车充电设施的网络化信息系统。它集成了充电设备的远程控制、状态监测、充电计费、用户管理、数据分析与报告等功能，旨在提高充电设施的利用率、安全性和用户体验。



充电设备 charging device

为新能源汽车提供电能补充的设备，包括充电桩、充电站、换电站等，它们通过电力电子技术和智能控制技术，将电能安全、高效地传输给新能源汽车的电池系统。



远程监控 remote monitoring

通过通信网络对充电设备的运行状态、工作参数、故障信息等进行实时监测和控制的技术手段。在充电平台管理系统中，远程监控是实现设备高效管理和维护的关键功能之一。



智能调度 intelligent dispatching

根据充电需求、设备状态、电网负荷等因素，通过算法和模型对充电资源进行动态分配和优化的过程。在充电平台管理系统中，智能调度可以提高充电设施的利用率，减少用户等待时间，平衡电网负荷。



数据分析与报告 data analysis and reporting

对充电平台管理系统收集的大量数据进行处理、分析和可视化的过程，以生成有意义的报告和洞察。这些报告可以用于评估系统性能、优化运营策略、预测未来趋势等，为决策者提供有力支持。



用户界面 user interface

充电平台管理系统与用户进行交互的视觉和操作界面，包括移动应用、网页端等。良好的用户界面设计可以提高用户的操作体验，降低使用难度，提升用户满意度。



安全性 safety

充电平台管理系统在保护用户信息、防止非法访问、抵御网络攻击等方面的能力。安全性是充电平台管理系统不可或缺的重要特性，直接关系到系统的稳定运行和用户的信任度。



互操作性 interoperability

充电平台管理系统与不同厂商、不同型号的充电设备以及其他相关系统之间能够顺畅地进行信息交换和协同工作的能力。互操作性是确保充电设施网络化和智能化的关键要素之一。

* 1. 系统组成
     1. 云平台层

云平台层负责数据的存储、处理和分析，基于智慧城市的大数据架构，能够实时接收和处理来自各个充电站点的数据，为用户提供智能化的服务。

关键组件包括数据中心、云计算平台、大数据处理模块等。

* + 1. 网络通信层

网络通信层负责实现系统各组件之间的数据传输和通信，采用先进的通信技术和协议，确保数据的实时性和可靠性。

关键组件包括有线网络、无线网络（如4G/5G）、物联网（IoT）通信模块等。

* + 1. 充电设施层

充电设施层是系统的前端，直接与用户的新能源汽车进行交互，提供各种类型的充电设备，以满足不同用户的充电需求。

关键组件包括充电桩、充电站、换电站等。这些设备需要具备智能感知、远程控制、状态监测等功能。

* + 1. 用户交互层

用户交互层是系统与用户之间的接口，负责提供直观、易用的操作界面和信息服务，支持多种终端设备，如手机、平板电脑、电脑等。

关键组件包括移动应用、网页端、自助服务终端等。组件应提供用户注册、充电预约、支付结算、充电记录查询等功能。

* + 1. 运营管理层

运营管理层负责系统的日常运营和管理，包括设备管理、用户管理、数据分析与报告等，支持多种运营模式，如自营、加盟等。

关键组件包括运营管理平台、客服中心、数据分析与报告模块等。组件应提供设备监控、故障报警、用户投诉处理、运营数据分析等功能。

* + 1. 安全防护层

安全防护层是系统的安全保障，负责保护用户信息和系统数据的安全，采用多种安全技术和措施，防止非法访问和数据泄露。

关键组件包括防火墙、入侵检测系统、数据加密模块等。组件需要提供身份认证、访问控制、数据加密、安全审计等功能。

* 1. 系统设计要求
     1. 开放性

系统应具有高度的开放性，支持各类硬件和网络系统，确保与不同品牌和型号的充电桩兼容。

采用国际标准协议，如TCP/IP、OSPF、IS-IS、SNMP等，确保系统的网络通信稳定性和安全性。

* + 1. 模块化与可扩展性

系统设计应采用模块化架构，便于功能的扩展和升级。

数据库设计应考虑数据的安全性、一致性和可扩展性，选择符合标准的数据库系统（如MySQL或MongoDB）进行数据存储。

预留接口，便于未来新技术或新需求的无缝接入。

* + 1. 稳定性与可靠性

系统应部署在云服务器上，利用云服务的高可用性优势，提升系统的整体性能和稳定性。

采用冗余设计和负载均衡技术，确保系统在高并发访问时的稳定性和响应速度。

定期进行系统维护和升级，及时处理用户反馈的问题和故障。

* + 1. 安全性

系统应采用加密技术保护用户数据的安全传输和存储，防止黑客攻击和数据泄露。

* 1. 功能要求
     1. 用户管理

提供用户注册、登录、个人信息管理等功能。

支持多角色管理，如普通用户、管理员、运营商等，并分配不同的权限和功能。

* + 1. 充电管理

支持充电桩的实时状态查询、预约、导航等功能。

提供多样化的计费模式，如按时间、消耗电量或充电速率计算，并支持在线支付和电子发票。

对充电记录、费用、设备使用频率等数据进行深度分析，生成可视化报表。

* + 1. 运维管理

支持充电桩的远程启停控制和参数调整，提升管理效率和响应速度。

提供故障预警和报警功能，及时通知运维人员处理充电桩故障。

对充电桩进行定期维护和保养，确保充电桩的正常运行。

* + 1. 数据分析与优化

对充电记录、用户行为等数据进行分析，为管理者提供决策支持。

通过数据分析优化充电策略，提升用户体验和充电效率。

支持定制化报告生成，满足不同用户的需求。

* + 1. 第三方平台接入

支持与政府监管平台、第三方支付平台等系统的互联互通，实现数据共享和业务协同。

提供API接口，便于其他系统或应用接入充电平台。

* + 1. 用户体验

界面设计应简洁明了，便于用户快速找到所需功能。

提供良好的用户引导和帮助文档，降低用户的学习成本。

持续优化系统性能，提升用户的使用体验。

* 1. 性能要求
     1. 系统响应时间

用户操作后，系统返回结果的时间。在正常情况下，系统响应时间应不超过3秒；在高并发情况下，系统响应时间应不超过5秒。

* + 1. 系统可用性

系统能够正常运行并提供服务的时间比例。系统可用性应不低于99.9%。

* + 1. 系统吞吐量

系统单位时间内能够处理的请求数量。在正常情况下，系统吞吐量应不低于每分钟处理1000个请求；在高并发情况下，系统吞吐量应不低于每分钟处理500个请求。

* + 1. 数据准确性

系统存储和展示的数据与用户实际操作的数据之间的误差率。数据准确性应不低于99.99%。

* + 1. 系统安全性

系统防止未经授权访问、数据泄露和破坏的能力。系统应通过国家相关安全认证，如等保三级或以上；系统应定期进行安全审计和漏洞扫描，确保没有已知的安全漏洞。

* + 1. 系统兼容性

系统能够与其他系统或设备进行数据交换和协同工作的能力。系统应支持多种操作系统和浏览器；系统应支持与不同品牌和型号的充电桩进行通信和数据交换。

* 1. 互联互通与兼容性要求
     1. 互联互通要求

系统应支持行业通用的通信协议，如TCP/IP、MQTT等，确保不同设备间能够顺畅通信。系统间交换的数据应采用统一的数据格式，如JSON、XML等，便于解析和处理。系统应提供标准化的API接口，供其他系统或应用调用，实现数据共享和功能协同。

系统应支持与其他充电平台或相关应用的用户账户互认，实现一键登录、信息共享等功能。系统应支持与第三方支付平台对接，实现支付功能的互联互通，方便用户支付充电费用。系统应支持与其他充电平台或充电桩运营商的充电服务协同，如充电桩预约、状态查询等，提升用户体验。

系统应支持与政府监管平台对接，实时上传充电数据、设备状态等信息，便于政府进行行业监管和数据分析。系统应支持按照政府要求，开放相关数据接口，供政府或其他机构进行数据分析和研究。

* + 1. 兼容性要求

系统应支持不同品牌、型号的充电桩接入，实现充电数据的统一管理和分析。系统应支持多种通信协议，确保与市场上主流充电桩的通信兼容。

系统应支持不同品牌、型号的电动汽车充电需求，提供适配的充电参数和策略。系统应支持国家标准的充电接口，确保与电动汽车的充电接口兼容。

系统应支持多种操作系统访问，如Windows、iOS、Android等，确保不同设备上的用户体验一致。系统应支持多种主流浏览器访问，如Chrome、Firefox、Safari等，确保网页展示和功能的正常。

系统应支持历史充电数据的迁移和导入功能，确保用户数据的连续性和完整性。系统应支持多种数据格式的导入和导出功能，如Excel、CSV等，便于用户数据的处理和分析。

* 1. 信息安全
     1. 系统平台安全

系统建设与运行应符合GB/T 20271、 GB/T 20273的安全技术要求。

信息安全级别应达到GB/T 22239第二级或以上的要求。

采用云计算系统架构时，系统安全服务能力应符合GB/T 31168的相关要求。

应建立系统身份认证机制，提供用户权限控制、系统应采取用户权限分级管理,角色职责与权限应清晰，各类用户必要时可采用实名认证。

应建立系统数据安全处理机制，数据的传输, 处理和存储应建立全过程安全控制。

应建立相应的信息安全运行体系，包括数据安全策略,如数据库安全、数据备份与恢复机制等,数据交换安全机制、应用安全策略保障、系统安全策略及网络安全策略等。

* + 1. 数据存储安全

应确保数据在传输过程中的安全，上传数据包可采用加密方式压缩，加密口令可由上下级相关平台约定。

应具有系统数据定期备份和灾难恢复机制,有条件者宜实行数据异地备份。

应定期进行用户数据清理和隐私保护，删除过期或冗余的数据,并采取必要的措施保护用户的个人隐私。

* 1. 实施与运维要求
     1. 实施要求

明确系统所需的服务器、存储设备、网络设备等硬件规格，以及网络环境要求，如带宽、延迟等。指定操作系统、数据库、中间件等软件的版本和配置要求，确保系统稳定运行。实施安全策略，包括数据加密、访问控制、防火墙设置等，保护系统免受攻击。

制定详细的数据迁移计划，包括数据源、目标、迁移时间、迁移方式等，确保数据完整性和一致性。建立定期数据备份机制，包括全量备份和增量备份，以及灾难恢复计划，确保数据安全。

对系统用户进行系统操作、功能使用等方面的培训，提高用户满意度和使用效率。提供7x24小时技术支持服务，及时解决用户在使用过程中遇到的问题。

* + 1. 运维要求

实施全面的系统监控，包括服务器性能、网络状况、应用响应时间等，及时发现并处理潜在问题。根据系统监控数据，定期对系统进行性能调优，确保系统在高并发、大数据量等情况下仍能保持高效运行。

建立故障排查流程，明确故障报告、分析、定位、修复等各个环节的责任人和时间要求。制定应急响应预案，针对系统故障、数据泄露等突发情况，快速启动应急响应机制，减少损失。

定期对系统进行安全审计，包括漏洞扫描、入侵检测等，确保系统安全性。实施权限管理策略，对系统用户进行分级授权，防止未授权访问和数据泄露。

定期对数据进行清洗、去重、格式化等操作，确保数据质量。利用大数据技术对数据进行分析和挖掘，为系统优化、业务决策提供支持。

