ICS 29.240.30
F 24

CES

团 体 标 准

T/CES XXX-XXXX

车网互动充放电设施信息安全防护技术规范

Technical specification for information security of electric vehicle charging-discharging facilities in vehicle-to-grid

（征求意见稿）

XXXX-XX-XX 发布　　XXXX-XX-XX 实施

中国电工技术学会发布

目　　次

前　　言.....20
1 范围.....1
2 规范性引用文件.....1
3 术语和定义.....1
4 信息安全防护总体要求.....2
4.1 防护框架.....2
4.2 防护原则.....3
4.3 防护目标.....3
5 充放电设施本体安全.....3
5.1 电动汽车充电系统安全.....3
5.2 充放电设备安全.....3
5.3 充电运营服务平台安全.....4
5.4 电网企业信息系统安全.....4
5.5 智能移动终端安全.....4
6 交互接口安全.....5
6.1 交互接口安全防护要求.....5
6.2 充放电设备与电动汽车交互接口安全.....5
6.3 充放电设备与充电运营服务平台交互接口安全.....5
6.4 充放电设备与智能移动终端交互接口安全.....5
6.5 充电运营服务平台与智能移动终端交互接口安全.....5
6.6 充电运营服务平台与电网企业信息系统交互接口安全.....5
6.7 充电运营服务平台与第三方平台交互接口安全.....5

前　言

本文件按照 GB/T1.1—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。

本文件由中国电工技术学会提出。

本文件由中国电工技术学会标准工作委员会能源智慧化工作组归口。

本文件起草单位：

本文件主要起草人：

本文件为首次发布。

车网互动充放电设施信息安全防护技术规范

1 范围

本文件规定了车网互动充放电设施信息安全技术要求，对车网互动中电动汽车充电系统、充放电设备、充电运营服务平台、电网企业信息系统、智能移动终端安全及交互接口安全提出了相关的技术要求。

本文件适用于车网互动中电动汽车充放电设施相关的信息安全防护设计、研发、测试评估和运行维护等。

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（包括所有的修改版）适用于本文件。

GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求

GB/T 41578—2022 电动汽车充电系统信息安全技术要求及试验方法

YD/T 3082—2016 移动智能终端上的个人信息保护技术要求

T/CEC 102.1 电动汽车充换电服务信息交换 第1部分：总则

T/CEC 102.2 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 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 电动汽车充换电服务信息交换 第4部分：数据传输及安全

T/CEC 208—2019 电动汽车充电设施信息安全技术规范

DL/T 2473.1—2022 可调节负荷并网运行与控制技术规范 第1部分：资源接入

DL/T 2473.2—2022 可调节负荷并网运行与控制技术规范 第2部分：网络安全防护

国家发展和改革委员会〔2014〕14号令 电力监控系统安全防护规定

国家能源局国能安全〔2015〕36号 电力监控系统安全防护总体方案等安全防护方案和评估规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

车网互动 vehicle-to-grid; V2G

指电动汽车和公共供电网间的能量互济双向流动过程。当电动汽车不使用时，车载电池的电能可通过充电桩传输给电网系统。如果车载电池需要充电，能量则由公共电网流向电动汽车车辆。

[来源：DL/T 2473.1—2022，3.12]

3.2

充放电设施 charging-discharging facilities

充电运营网络中提供充放电服务的设施，包括电动汽车充电系统、充放电设备、充电运营服务平台、电网企业信息系统、智能移动终端等。

3.3

电动汽车充电系统 charging system of electric vehicle

电动汽车车内，用于动力电池充放电的相关功能系统。根据充电方式及技术架构的不同，可能包含一个或多个车载控制器，例如电池管理系统、车载充电机、无线充电系统，或其他集成相关充放电功能的车载通信控制单元。

3.4

充放电设备 charging-discharging equipment

承担充放电服务功能的交直流充放电设备以及配套设备，与电动汽车或动力蓄电池相连接，并为其提供电能或接受其电能。

3.5

充电运营服务平台 charging operating service platform

充电运行网络中承担后台充放电服务功能的运行和提供信息服务的系统，是连接电动汽车用户、电动汽车、充放电设备、服务提供商的互联网信息服务平台，实现电动汽车充电、放电、租赁和交易的客户侧服务业务等。

3.6

电网企业信息系统 information system of power grid enterprise

电网企业侧涉及车网互动的信息系统，如负荷调控系统、电力市场交易系统、电力负荷管理系统等。

3.7

智能移动终端 intelligent mobile terminal

电动汽车用户使用的承载充放电应用软件的移动终端、充电设施运维人员使用的承载充电桩运维软件的移动运维终端。

4 信息安全防护总体要求

4.1 防护框架

车网互动充放电设施信息安全防护框架如图1所示。防护对象包含电动汽车充电系统（用户层）、智能移动终端（用户层）、充放电设备（充放电运营服务层）、充电运营服务平台（充放电运营服务层）、电网企业信息系统（电网层）的本体及相互间的接口，并支持可扩展。

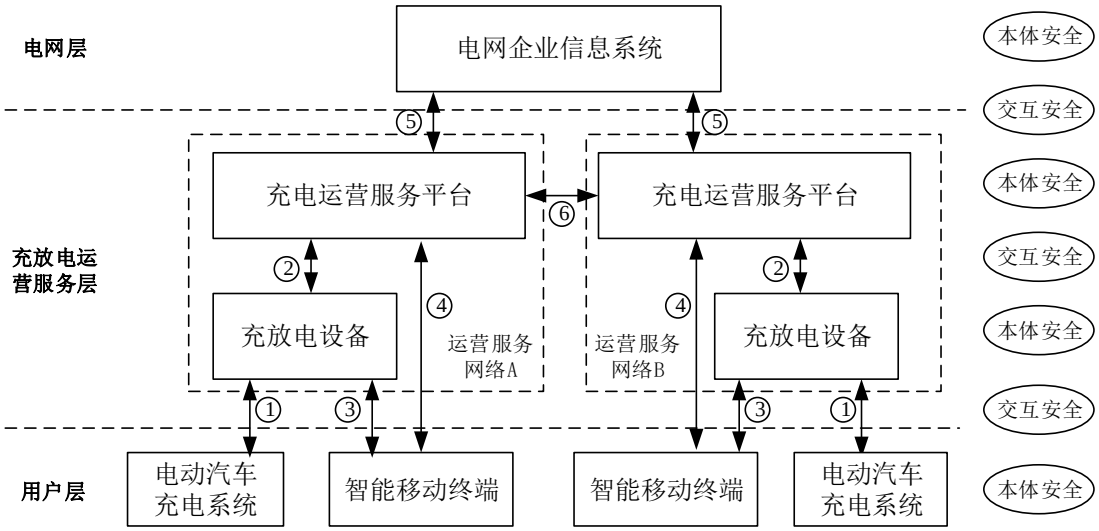

图1 车网互动充放电设施信息安全防护框架

4.2 防护原则

车网互动充放电设施信息安全防护原则包括：

a) 充放电设施信息安全防护必须严格遵守国家、行业相关法律、标准、规范的规定；
b) 坚持安全要求具备可操作性，切实指导系统设计、实施、运行工作；
c) 优先应用成熟的安全防护技术和产品，继承已有信息安全工作成果，紧跟信息安全和业务发展趋势；
d) 应对充放电设施上线前、中、后进行全生命周期信息安全风险评估，并制定相应应急响应机制；
e) 应开展数据分类分级防护，数据在对外提供、公开发布、跨域传输等环节前应采取数据内容防泄漏、数据脱敏等技术措施。

4.3 防护目标

车网互动充放电设施信息安全防护目标包括充放电设施本体安全、交互接口安全两部分，具体如下：

a) 充放电设施本体安全：保护电动汽车充电系统、充放电设备、充电运营服务平台、电网企业信息系统、智能移动终端安全可靠运行、免受恶意攻击。
b) 交互接口安全：充放电设施本体、接口进行信息交换过程中，保护数据在传输、处理、存储过程中不被泄漏、破坏和未授权使用等。

5 充放电设施本体安全

5.1 电动汽车充电系统安全

电动汽车充电系统安全包含硬件安全、软件安全、数据安全、通信安全，应确保电动汽车在充电、非充电（静置/运行）状态中个人隐私、充电数据、车内数据等安全，其技术要求及试验方法应参照GB/T 41578-2022执行。

5.2 充放电设备安全

5.2.1 充放电设备部署在开放环境中，应包含物理安全、本体安全。

5.2.2 物理安全方面具体要求如下：

a) 充放电设备应在柜门采用双重锁具机制；
b) 充放电设备宜通过视频摄像头等装置进行实时监测；
c) 设备现场调试过程应设立现场行为规范，用于规范现场维护过程的行为，并对违规行为和潜在故障行为进行识别与研判。

5.2.3 本体安全方面，应包括身份鉴别、访问控制、数据安全、通信安全、入侵防范、安全审计、备份恢复、可信验证，具体要求如下：

a) 身份鉴别过程应具有唯一性标识，宜采用基于国密算法的密码技术进行身份鉴别；
b) 应建立动态访问控制机制，通过制定动态的安全访问控制策略实现对充放电控制核心模块的访问控制，调整充放电设备对资源的访问权限。
c) 应采用基于国密算法的密码技术支持的保密机制或建立安全运行环境，且对数据进行加密后传输，所使用的密钥或数字证书应由国网统一密码服务平台颁发；
d) 充放电设备的核心计费控制模块应使用专用的 SIM 卡进行通信；
e) 具备发现设备上进程异常行为的能力，如非法访问端口，非法访问文件等，并具备自动阻断该非法行为的能力；
f) 支持对各类系统事件、非正常行为以及操作事件的审计及记录；
g) 充放电设备的重要文件应定期使用文件完整性检查工具或脚本对重要文件进行完整性检测和恢复验证；
h) 可基于可信根对充放电设备的核心计费控制模块的引导程序、系统程序、重要配置参数和应用程序等进行可信验证。

5.3 充电运营服务平台安全

5.3.1 充电运营服务平台系统防护应参照GB/T 22239-2019中第三级标准执行，应包括物理防护、边界防护、网络防护、应用防护、数据防护和主机防护。

5.3.2 充电运营服务平台用于生成式人工智能产品的预训练、优化训练数据，应符合《中华人民共和国网络安全法》等法律法规要求，能够保证数据真实性、准确性、客观性、多样性，包含个人信息的，应取得个人信息主体同意或者符合法律、行政法规规范的其他情形。

5.3.3 利用生成式人工智能产品应当安全可靠，应采取数据投毒分析、算法后门监测等措施，防止人工智能产品中植入恶意数据、代码。

5.4 电网企业信息系统安全

5.4.1 电网企业信息系统防护设计应满足国家发改委 14 号令和国家能源局国能安全〔2015〕36 号文“安全分区、网络专用、横向隔离、纵向认证”的防护原则建立格栅状安全防护架构，系统防护参照 GB/T 22239-2019 中第三级 标准执行，应包括物理防护、边界防护、网络防护、应用防护、数据防护、主机防护。

5.4.2 电网企业信息系统中负荷调控系统控制功能应在生产控制大区设计单独子分区，与生产控制区中原有系统逻辑隔离，负荷调控系统管理功能、电力市场交易系统、电力负荷管理系统应部署在管理信息大区，有外网交互功能的应用应将前端部署在互联网大区，将数据库部署在管理信息大区，通过边界逻辑强隔离设备交换数据。

5.5 智能移动终端安全

5.5.1 智能移动终端安全防护可参照 T/CEC 208-2019 执行，应包括运行机制安全、应用安全、恶意行为防范；

5.5.2 智能移动终端应具备多属性身份认证功能，对登录用户进行增强型身份标识和鉴别，个人信息保护可参照 YD/T 3082-2016 执行；

5.5.3 智能移动终端应支持动态访问控制权限调整，对终端数据、终端资源访问权限可根据用户信任等级进行动态调整。

6 交互接口安全

6.1 交互接口安全防护要求

车网互动中电动汽车充电系统、充放电设备、充电运营服务平台、电网企业信息系统、智能移动终端之间网络环境开放，为降低资源访问过程中的安全风险，彼此之间的交互应以数字身份为基础，在访问被允许之前进行身份认证和授权，在一次端到端的资源访问全生命周期中，持续对动态变化的多源信息进行信任评估，以最小访问权限为原则，进行动态访问控制资源按需分配。

6.2 充放电设备与电动汽车交互接口安全

充放电设备与电动汽车之间的信息交互接口安全包括通信网络安全、数据安全、传输通道安全，重点防护避免仿冒获取和控制充电控制信息，应对物理接口、现场电缆和无线网络通信等进行监测和管理。

6.3 充放电设备与充电运营服务平台交互接口安全

充放电设备与充电运营服务平台之间的信息交互接口安全包括设备认证安全、数据安全、通信网络安全、传输通道安全，重点防护基于互联网链路下的数据通信网络和控制信息安全，应对充电设备远程通信协议格式、交互机制、异常监测和处理流程等进行监测和管理。

6.4 充放电设备与智能移动终端交互接口安全

充放电设备与智能移动终端之间的信息交互接口安全包括身份认证安全、服务认证安全、数据安全、传输通道安全，重点防护在充放电设备现场环境下，不同终端或凭证在身份认证和业务认证过程信息的保密性、完整性和可用性，应对通信协议格式和数据规范等进行监测和管理。

6.5 充电运营服务平台与智能移动终端交互接口安全

充电运营服务平台与智能移动终端之间的信息交互接口安全包括身份认证安全、服务认证安全、数据安全、传输通道安全，重点防护在互联网环境下，不同终端或凭证在身份认证和业务认证过程信息的保密性、完整性和可用性，应对通信协议格式和数据规范等进行监测和管理。

6.6 充电运营服务平台与电网企业信息系统交互接口安全

充电运营服务平台与电网企业信息系统的信息交互接口安全包括身份认证安全、数据安全、审计安全，充电运营服务平台与电网企业信息系统通信时应进行访问控制、身份认证、数据加密与日志审计等措施，重点防护项：

a）在建立数据连接之前进行身份认证；

b）采用国密算法保证鉴别信息和重要业务数据等敏感信息在传输过程中的保密性和完整性；

c）对交互数据进行日志审计。

6.7 充电运营服务平台与第三方平台交互接口安全

应满足T/CEC 102.1、T/CEC 102.2、T/CEC 102.3、T/CEC 102.4中平台鉴权认证、数据传输安全、信息隐私保护、密钥使用及管理等相关要求。