ICS35.240.50
CCSL77

团体标准

T/CESXXX-2024

电力作业现场智能化安全管控系统

第 4 部分：数据管理与分析技术规范

Intelligent safety management and control system at electric power operation site

—Part4:Technical specification for data management and analysis

20XX-XX-XX 发布 20XX-XX-XX 实施

中国电工技术学会发布

目次

前言

为了提高标准的适用性，完善《电力作业现场智能化安全管控系统》系列团体标准体系，在已有 3 部分的基础上新增第 4 部分，具体如下：

——第 1 部分：总则；

——第 2 部分：现场管控终端技术规范；

——第 3 部分：智能服务技术规范；

——第 4 部分：数据管理与分析技术规范。

本文件是《电力作业现场智能化安全管控系统》的第 4 部分。

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。

本标准由国网信息通信产业集团有限公司提出。

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。

本标准起草单位：国网信息通信产业集团有限公司、福建亿榕信息技术有限公司、国家电网有限公司、福州大学、国网福建省电力有限公司、国网福建省电力有限公司南平供电公司、国网福建省电力有限公司三明供电公司、国网福建省电力有限公司电力科学研究院、湖北华中电力科技开发有限责任公司、北京国网信通埃森哲信息技术有限公司。

本标准主要起草人：李强、庄莉、王罡、陈铭、王秋琳、严士华、邬群勇、陈伯建、梁懿、黄长协、汪小钦、邵海明、李蒙蒙、赵楷、李炳森、黄建业、吕君玉、伍臣周、王从、刘茂凯、陈瑞洪、林晨翔、林福飞、吴尔燮、漆启华、张财强、林爽、刘杰、余世煌、熊嘉丽、蔡欣溢、施国忠、叶文良。

本标准为首次发布。

电力作业现场智能化安全管控系统
第 4 部分：数据管理与分析技术规范

1 范围

本标准规定了电力作业现场智能化安全管控系统的数据管理与分析技术规范，包括总体要求，以及数据采集接入、数据处理融合、数据组织存储、数据挖掘应用、数据归档共享、数据销毁、数据安全和隐私保护要求。

本标准适用于电力作业现场智能化安全管控系统的设计、开发、测试和部署等环节。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是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—2019 信息安全技术 网络安全等级保护基本要求

GB/T 34960.5 信息技术服务 治理 第 5 部分：数据治理规范

GB/T 36073—2018 数据管理能力成熟度评估模型

T/CES 131—2022 电力作业现场智能化安全管控系统 第 1 部分：总则

T/CES 132—2022 电力作业现场智能化安全管控系统 第 2 部分：现场管控终端技术规范

T/CES 133—2022 电力作业现场智能化安全管控系统 第 3 部分：智能服务技术规范

3 术语和定义

T/CES 131—2022 界定的以及下列术语和定义适用于本文件下列术语和定义适用于本文件。

3.1

统一物联资源管理平台 unified iot resource management platform

包括统一视频平台、物联管理平台，作为云端系统服务，具备边端设备台账资源管理、运行状态监测与控制、数据采集汇聚，以及为云端其他系统提供边端设备调控等服务。

3.2

统一视频平台 unified video platform

应用于电网建设管理、生产管理、应急指挥等方面，为业务系统提供音视频、告警等信息的远程采集、传输、存储、控制等功能的视频监控与管理平台。

3.3

物联管理平台 iot management platform

对上通过标准化接口向智能服务等系统提供服务；对下以标准物联网协议或电力专用物联网协议，与现场管控终端、现场智能终端等进行交互，实现各类终端的统一接入和管理。

3.4

人工智能平台 artificial intelligence platform

一套集成了人工智能算法、数据处理工具、模型训练和部署能力的软件系统。具备样本库、模型库、运行平台、训练平台等功能模块。

3.5

安全接入平台　safe access platform

具备提供安全、可控的网络接入解决方案的系统，确保所有连接到企业局域网的设备、用户和应用程序都经过验证、授权和加密。

3.6

本体软件　ontology software

指运行在特定现场管控终端上的应用软件，具备对终端运行状态监控能力，依托终端对外提供服务。

3.7

视频监控类设备　video surveillance equipment

指具备视频采集、传输功能的移动布控球、围栏摄像机等终端设备。

3.8

数据生存周期　data life cycle

数据获取、存储、整合、分析、应用、呈现、归档和销毁等各种生存形态演变的过程。

[GB/T 34960.5，定义 3.7]

3.9

数据安全　data security

数据的机密性、完整性和可用性。

[GB/T 36073—2018，定义 3.11]

4　缩略语

下列缩略语适用于本文件。

CoAP：受限应用协议 (constrained application protocol)

FTP：文件传输协议（file transfer protocol）

HTTP：超文本传输协议（hypertext transfer protocol）

HTTP（S）：超文本传输安全协议（hypertext transfer protocol(secure)）

JSON：JavaScript 对象表示法（java script object notation）

LoRa：基于线性扩频的远距离通信技术的远距离无线传输技术（long range radio）

LoRaWAN：LoRa 远距离通信网络设计的一套通讯协议和系统架构（long range wide area network）

MQ：消息队列（message queue）

MQTT：消息队列遥测传输（message queuing telemetry transport）

MySQL：关系型数据库管理系统（my structured query language）

ONVIF：开放式网络视频接口论坛（open network video interface forum）

OSS：对象存储服务（object storage service）

RFID：无线射频识别技术（radio frequency identification）

SQL：结构化查询语言（structured query language）

SSL：安全套接层（secure sockets layer）

TLS：传输层安全性协议（transport layer security）

UUID：通用唯一识别码（universally unique identifier）

WIFI：基于 IEEE 802.11 标准的无线局域网通信技术（wireless fidelity）

5 总体要求

电力作业安全生产是人民生命安全、国家能源安全和社会经济发展的重要保障。电力作业现场数量多、作业人员多、专业配合多，各类安全风险和事故隐患交织叠加，安全管控难度大，通过信息系统平台和智能安全终端实施远程监控和现场管控的模式，已无法适应“作业、风险”两多趋势下安管要求。创新构建云边端协同的作业现场与远端管控相结合的高效智能协同安全管控技术体系，提升电力现场作业安全管控水平，是未来电力作业安全管控发展的必然趋势。

5.1 数据总体架构

电力作业现场智能化安全管控系统的总体架构应符合 T/CES 131—2022 的规定，由智能服务、现场管控终端和现场智能终端组成，采用“云、边、端”协同的应用架构。云侧智能服务从业务系统获取业务数据，第三方平台获取模型数据，整合内部的业务应用、管理应用需求，形成现场作业管控业务数据下发至边侧现场管控终端；边侧现场管控终端接收到云侧业务数据后，通过搭载的人工智能模型，针对汇聚端侧各类感知数据进行作业违章风险分析，并将分析结果、端侧的感知数据通过本体软件上传至云侧智能服务；端侧现场智能终端接收到边侧现场管控终端对终端设备查询、控制指令后，将所采集的视频、图像、定位及传感等数据上传汇聚至边侧现场管控终端。电力作业现场智能化安全管控系统数据架构如图 1 所示。

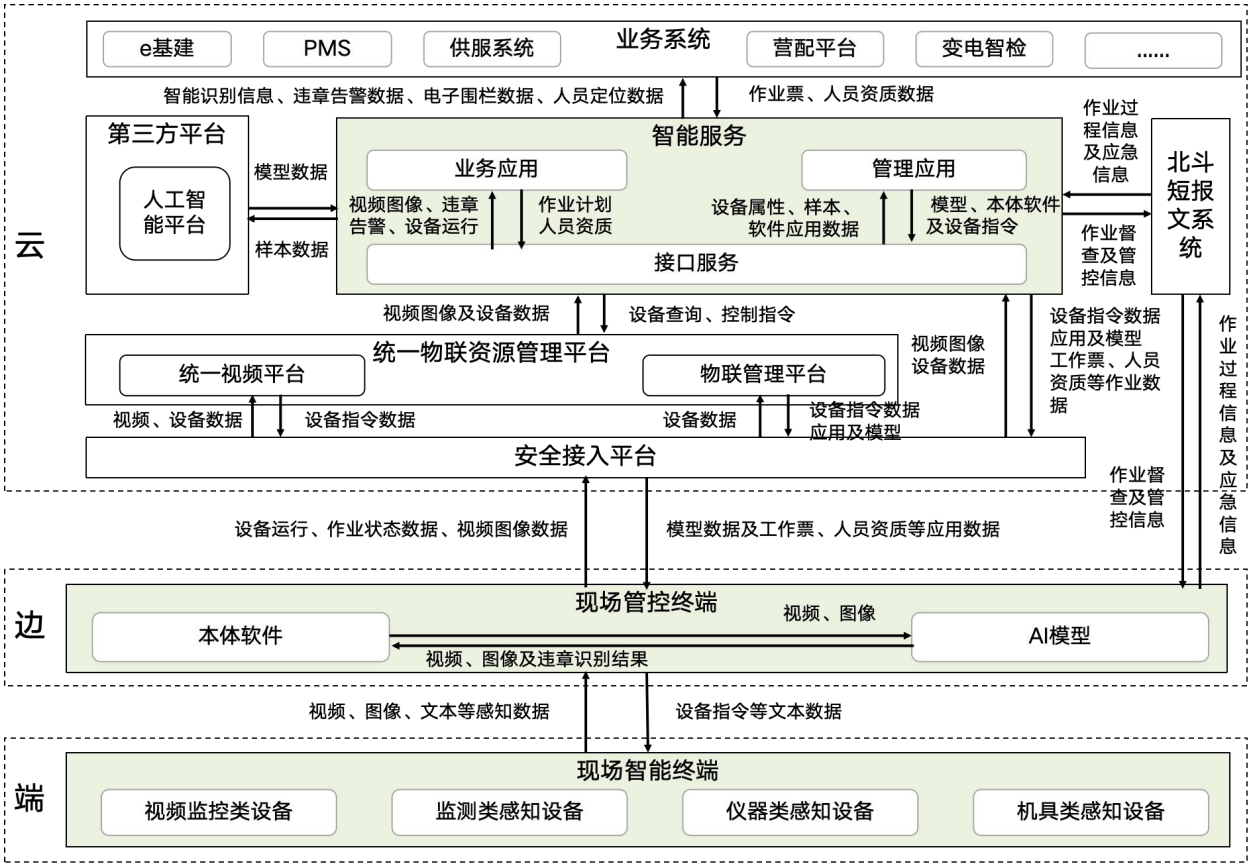

图 1 电力作业现场智能化安全管控系统数据架构

a） 云侧智能服务与各系统交互数据流转

1) 在与业务系统交互过程中，应具备将智能识别信息、违章告警数据、电子围栏数据、人员定位数据等业务数据上传至 e 基建、PMS、供服系统、营配平台、变电智检等业务系统，以及具备接收业务系统下发的作业票、人员资质等作业数据；
2) 在与第三方平台交互过程中，应具备将现场作业违章视频、图像等数据上传至人工智能平台等系统中，以及具备接收人工智能平台下发的人工智能模型；
3) 在与统一物联资源管理平台交互过程中，应具备下发设备信息查询、控制指令至统一视频平台、物联管理平台等系统，以及具备接收统一视频平台、物联管理平台发送的设备基础信息、运行状态信息及现场作业视频图像等数据；
4) 在与北斗短报文系统交互过程中，应具备现场督查、管控信息下发至北斗短报文系统，以及具备接收现场作业过程及应急信息等数据。

b）边侧现场管控终端与各系统交互数据流转

1) 在与云侧智能服务交互过程中，一是应具备通过安全接入平台、统一物联资源管理平台将设备运行数据、作业状态数据、作业视频图像等数据上传至云侧智能服务，以及具备通过统一物联资源管理平台、安全接入平台接收云侧智能服务下发的人工智能模型、软件应用及工作票、人员资质等应用数据。二是应具备直接通过安全接入平台将设备运行数据、作业状态数据、作业视频图像等数据上传至云侧智能服务，以及应具备通过安全接入平台接收云侧智能服务下发的人工智能模型、软件应用及工作票、人员资质等应用数据；
2) 在与北斗短报文系统交互过程中，应具备将现场作业过程及应急信息等数据发送至北斗短报文系统，以及接收北斗短报文系统下发的作业督查及管控信息等。

c）端侧现场智能终端与各系统交互数据流转

1) 在与边侧现场管控终端交互过程中，具备将各类终端设备采集的视频、图像、定位及传感等感知数据上传至现场管控终端，以及具备接收现场管控终端下发的设备信息查询、控制指令等文本数据。

5.2 数据管理框架

综合考虑电力作业现场智能化安全管控系统云侧、边侧、端侧数据来源、类型、用途等因素，对系统数据进行分类分层，按照一定的数据管理原则和数据安全隐私保护，对系统数据的采集接入、处理融合、组织存储、挖掘应用、归档共享、销毁的数据生存周期进行管理。电力作业现场智能化安全管控系统数据管理框架如图 2 所示。

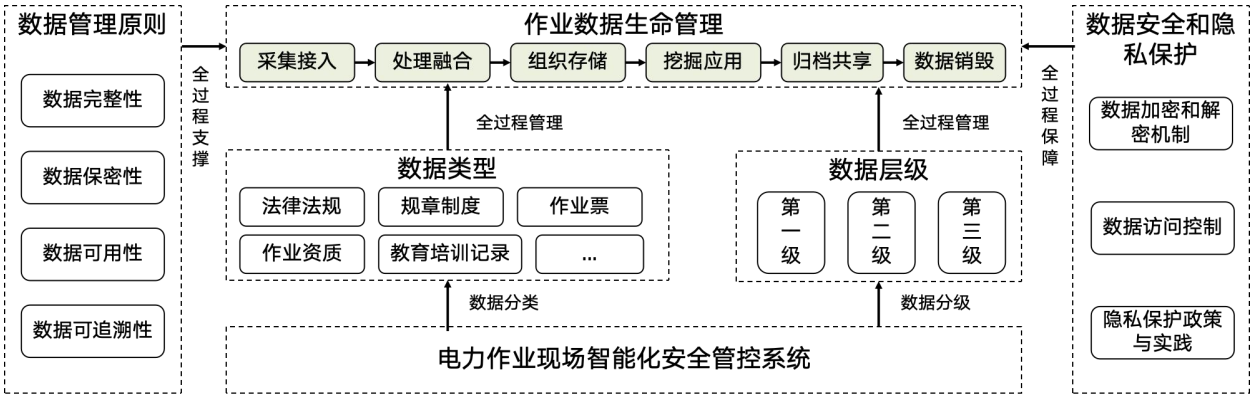

图 2 电力作业现场智能化安全管控系统数据管理框架

5.2.1 数据分类和分级

应根据电力现场作业云、边、端数据的来源、性质、内容、敏感性和重要性，对数据进行分类和分级，制定相应的管理策略。

a）数据分类

应根据电力现场作业数据的性质与内容对电力现场作业数据进行分类，包括但不限于：

1) 法律法规：应包含国务院、能源局、发改委等政府单位发布的与电力安全生产作业相关的法律法规文档。例如，安全生产法、数据安全法、特种设备安全法、施工监督管理办法等；
2) 规章制度：应包含电力企业发布的电力现场作业安全管控相关的管理办法、管理规定、工作规范、工作规程。例如，电力作业安全监督管理办法、安全工作规定、安全生成风险管控管理办法、安全工作奖惩规定、安全工作规程等；
3) 作业票：应包含电力企业规范开展现场施工、检修作业相关的流程文档。例如，工作票、操作票、现场勘察记录、安全技术交底、检修方案、标准作业卡、现场安全交底会记录卡等；
4) 作业资质：应包含电力施工单位、队伍人员规范开展施工、检修作业所需具备的资质证书、技能证书。例如，电力设施许可证、安全生产许可证、建筑企业资质证、特种作业操作证等；
5) 作业现场数据：应包含电力现场施工作业过程产生的管控数据。例如现场作业视频图像、现场感知数据、违章告警数据等；
6) 教育培训记录：应包含电力施工队伍人员参与的作业安全、作业技能教育培训相关数据。例如电力作业安规考试、现场作业实训等。

b）数据分级

应根据电力现场作业数据的敏感性、重要性和对业务连续性、安全性影响程度对数据进行分层级，包括但不限于：

1) 第一级：应是能够公开发布、删除后不影响系统正常运行的电力现场作业数据。例如，公开发布的法律法规、规章制度、系统常规操作日志等；
2) 第二级：应是仅在电力企业内部发布、实时作业生产数据及影响业务连续性的电力现场作业数据。例如，电力企业发布的内部规章制度、作业票、现场作业数据等；
3) 第三级：应是涉及作业队伍人员隐私、电力企业专有及涉密的电力现场作业数据。例如，作业资质数据、作业队伍教育培训记录、作业人员违章信息等。

6 数据管理原则

电力作业现场智能化安全管控系统应遵循但不限于数据完整性、数据保密性、数据可用性和数据可追溯性的数据管理原则。

a）数据完整性原则：

应符合 GB/T 22239—2019 中数据完整性要求，并符合以下要求：

1) 应通过设置完整性约束和规则，防止系统与业务系统、北斗短报文系统、第三方平台等外部系统及智能服务、现场管控终端、现场智能终端内部模块交互过程中不完整或无效数据的输入；
2) 应采用哈希算法、数字签名、校验等技术手段，确保端侧现场智能终端、边侧现场管控终端、云侧智能服务数据在传输和存储过程中不被篡改；
3) 应建立数据完整性监控机制，对任何试图违反系统数据准确、一致、未经授权不被更改等特性的行为进行检测和告警；

4) 应实施统一的数据标准和规范，包括但不限于样本模型命名规则、样本标注规则、模型构建打包规则、数据模型、数据交互传输协议；
5) 应定期对云侧智能服务汇聚业务数据，包括但不限于现场违章风险数据、作业队伍人员资质、终端设备属性等数据进行质量评估，及时发现并纠正错误或不一致的数据。

b）数据保密性原则：
1) 应确保只有经过授权的用户和外部系统才能够访问系统云边端数据；
2) 应实施基于角色的访问控制（RBAC）和最小权限原则，为不同级别的用户分配适当的访问权限，用户类型包括但不限于现场一线班组、作业督察人员、安全管控人员、安全决策人员；
3) 应对系统智能服务、现场管控终端、现场智能终端模块在不同部署与使用环境下采用不同加密技术对数据进行存储、传输，以防止数据在未经授权的情况下被读取或篡改；
4) 应在非生产环境中使用数据时，对施工单位资质、人员身份与作业证书等敏感数据进行脱敏处理，以隐藏或替换个人身份信息；
5) 应实施实时系统监控和日志记录，检测和报告任何未经授权的数据访问或异常行为。

c）数据可用性原则：
1) 应对作业票、作业资质、作业过程等系统业务数据实施备份策略，包括定期的全量备份和增量备份，以减少数据丢失的风险；
2) 应监控和优化云端智能服务数据库和数据处理系统的性能，确保快速响应前端违章风险等信息的访问和查询请求；
3) 应采用缓存、索引和数据分区等技术手段，提高海量异构的文本、视频、图像等作业数据关联检索和处理的速度；
4) 应提供多种访问方式和接口，以便一线班组、督察监管人员等用户可以通过不同的设备和平台访问数据；
5) 应确保数据格式和协议的标准化，以便数据可以在不同的系统和应用之间无缝集成。

d）数据可追溯性原则：
1) 应在智能服务、现场管控终端本体软件中启用详细的审计日志记录功能，记录所有数据访问、修改和删除活动；
2) 应确保审计日志包含足够的信息，包括但不限于用户身份、时间戳、操作类型和受影响的数据内容；
3) 应对样本、模型、应用软件及作业业务数据和各类规章制度文档等实施版本控制，记录每次变更的详细信息，包括但不限于变更原因和变更者；
4) 应为样本、模型、违章风险等数据添加标签和元数据，包括但不限于创建者、创建日期、来源、敏感级别、基础属性，以增强数据的可追溯性；
5) 应建立数据流向图和追踪机制，以便在发生安全事件或合规审查时，可以快速定位数据的来源和去向。

7 数据采集接入

7.1 智能服务数据接入

a）应支持 MQTT、HTTP 等通信协议；
b）应支持北斗短报文通信功能；
c）应具备向业务系统推送作业数据，以及接收工作票、人员资质等数据并下发至现场管控终端的能力；

d）应支持接入安全接入平台；
e）应支持向第三方平台推送样本数据，并能接收模型数据的能力。

7.2 现场管控终端数据接入

a）应具备 WIFI、LoRa、蓝牙、以太网、4G\5G 等通信接口；
b）应支持 MQTT、Modbus-TCP 、LoRaWAN、CoAP 等通信协议；
c）宜具备安全加密模块，能够独立接入安全接入平台；
d）应支持北斗短报文通信功能；
e）应具备定时上报现场管控终端版本、电量等信息的能力，数据上报频率应不低于每 5 分钟 1 次；
f） 现场产生新的作业数据时，应实时上报智能服务；
g）应具备接收智能服务下发的工作票、人员资质等信息的能力；
h）网络带宽应不低于 100Mbps。

7.3 现场智能终端数据采集

7.4 作业现场中智能终端应至少包含 1 个视频监控类设备，以及 2 个定位类设备，其余设备根据现场情况提供。

7.4.1 视频监控类设备

应支持包括各种移动布控球、围栏摄像机等视频监控类设备的数据采集，应符合以下要求：
a）宜具备安全加密模块，能够独立接入安全接入平台；
b）应支持 WIFI、4G\5G 等通信接口；
c）应支持 ONVIF 协议中的媒体服务、云台服务规范，实现视频传送及云台控制功能。

7.4.2 定位类设备

应支持包括融合定位终端、无线脉冲定位标签等定位类设备的数据采集，应符合以下要求：
a）应具备 WIFI、LoRa、蓝牙、以太网、4G/5G 其中至少一项通信接口；
b）应支持 MQTT、Modbus-TCP、LoRaWAN、CoAP 其中至少一项通信协议；
c）应具备定时上报设备状态、电量信息的能力，数据上报频率应不低于 1 次/秒；
d）融合定位终端应支持接收现场管控装置下发的文字信息并进行语音播报；
e）设备状态发生变化时，应实时上报数据。

7.4.3 传感器类设备

应支持包括气体检测仪、智能接地线、倾角传感器等传感器类设备的数据采集，应符合以下要求：
a）应具备 WIFI、LoRa、蓝牙其中至少一项通信接口；
b）应支持 MQTT、Modbus-TCP、LoRaWAN、CoAP 其中至少一项数据通信协议；
c）应具备定时上报传仪器检测数据、电量信息的功能，且上报频率应不低于每 5 分钟 1 次；
d）仪器检测数据超过指定阈值时应实时上报数据；
e）应具备接收检测指令，并实时上报仪器检测结果的功能。

8 数据处理融合

8.1 智能服务数据处理

8.1.1 工作票数据处理

a）应采用 JSON 的格式进行数据传输，方便数据的转换和解析；
b）针对工作票的内容，应制定统一的数据字典，例如作业专业字典、班组人员类型字典；

c） 针对工作票票的班组人员信息，应提取人员信息做分表存储和支撑界面的班组人员管理，并对人员的人脸图片进行下载和转存；
d） 工作票下发现场管控终端时，应制定唯一标识编码；
e） 当现场管控终端接收成功后，应返回接收成功标识和唯一标识编码；
f） 针对未接收成功返回的唯一标识编码，应制定重复推送逻辑，直至收到成功标识。

8.1.2 现场业务数据处理

a） 针对不同场景类型的业务数据，应制定不同编码分类入口来接收数据，并做对应的处理逻辑；
b） 针对业务现场的图片类数据，应将图片文件存放到对象存储服务中，并根据不同类型的对象存储制定不同逻辑的存取方式。

8.2 现场管控终端数据处理

8.2.1 工作票数据处理

a） 应在接收到下发的工作票数据时，立即返回接收成功编码和唯一性标识；
b） 应对收到的工作票进行格式解析，并将解析后的数据推送给单兵掌机，支撑现场作业。

8.2.2 现场业务数据处理

a） 应对智能终端上传的数据进行解析，对冗余数据制定明确的格式，方便展示和读取；
b） 应对视频类终端制定统一格式的控制指令；
c） 应对现场作业的业务数据进行二次确认逻辑处理，避免产生冗余数据。

9 数据组织存储

9.1 云端数据存储

云端数据应存储在管理信息内网中，可以确保数据的安全性、可靠性、集中管理和符合行业规范等要求，是保障电力系统稳定运行和高效管理的重要措施。

9.1.1 结构化数据存储

a） 应根据业务需求和数据特点选择合适的数据库类型，如关系型数据库（MySQL）；
b） 应设计合理的数据模型和关联关系，更好的保存边端台账数据、边端运行数据、违章告警数据、电子围栏数据、人员定位数据、作业票数据、人员数据、模型数据等；
c） 对于有上云要求的，应满足对云平台数据库组件的兼容适配。

9.1.2 非结构化数据存储

a） 应使用对象存储服务来保存非结构化数据，人脸图片、违章图片、模型文件等应放置在不同的目录下；文件名应带有年月日信息，方便整理和查找；文件名应采用通用唯一标示符（UUID），防止重复和被爬取；
b） 对于有上云要求的，应满足对云平台对象存储组件的兼容适配。

9.2 边端数据存储

9.2.1 结构化数据存储

a） 为加快边端服务启动，减少使用等待时间，应使用轻量级和快速的数据库，如国产关系型数据库（Kingbase）；
b） 应设计合理的数据模型和关联关系，更好的保存违章类型数据、违章规则数据、工器具数据、违章告警数据、电子围栏数据、作业票数据、人员数据、模型数据等。

9.2.2 非结构化数据存储

a）应使用边端自身的服务器来保存非结构化数据；人脸图片，违章图片，模型文件等应放置在不同的目录下；文件名应带有年月日信息，方便整理和查找；文件名应采用通用唯一标示符（UUID），防止重复和被爬取；
b）对于需要上传云端的非结构化数据，应调用云端的非结构化数据存储服务接口，把非结构化数据保存一份到云端的非结构化数据存储服务中；
c）对于需要下载云端的非结构化数据，应调用云端的非结构化数据存储服务接口，从云端的非结构化数据存储服务中下载保存到自身的服务器中。

10 数据挖掘应用

10.1数据场景支撑

10.1.1 支撑人员资信准入核验

应用获取人员数据支撑现场人员资质查看、身份核实、安全准入判定等资信准入核验功能，应符合以下要求：

a）应可查看作业计划关联相关人员(包括工作负责人、工作票签发人、工作许可人、班组成员等)基本信息；
b）应可查看人员作业资质信息，并与人员资质准入信息保持一致；
c）应可查看人员安规考核成绩、履历信息、违章信息；
d）应具备现场人员人脸数据验证功能；
e）应具备现场人员准入异常告警功能；
f） 应具备现场作业人员数量异常比对功能。

10.1.2 支撑软件版本管理与统计

应采集应用版本数据，支撑软件版本信息维护管理功能，应符合以下要求：

a）应具备根据软件版本命名规则维护及更新版本信息的功能；
b）应具备以远程及离线方式进行版本部署与升级的功能；
c）应具备各软件版本在用数量统计功能。

10.1.3 支撑样本汇总与分类

应具备样本数据汇总与分类功能，应符合以下要求：

a）应具备样本图片上传云端边缘智能服务平台汇总管理功能；
b）应具备样本图片数据分类维护功能。

10.1.4 支撑数字化作业统计分析

应具备智能终端应用次数统计功能，支撑数字化作业应用统计，应符合以下要求：

a）应具备智能终端与作业计划关联的记录；
b）应具备按照时间范围、区域范围统计智能终端与作业计划的关联次数。

10.1.5 支撑工器具进出场检查

应具备对现场工器具进出场的数据采集功能，支撑工器具进出场数量检查功能，应符合以下要求：

a）应支持以 RFID 或 APP 扫码方式获取现场工器具信息的功能；
b）应具备工器具遗漏检查功能。

10.1.6 支撑电子围栏管理

应具备北斗定位数据采集并行成电子围栏区域的功能，支撑电子围栏绘制、展示等功能，应符合以下要求：

a）应具备通过融合定位终端定位数据对作业区域、危险区域绘制以及特殊区域（基坑、电线杆等）标注功能；

b）应具备作业区域出入口设置功能；
c）应具备多区域电子围栏绘制以及已绘制电子围栏调整功能；
d）应具备电子围栏地图缩放、网格设置、指北针、比例尺功能。

10.1.7 支撑定位与布控球联动抓拍

应具备定位数据采集功能，支撑布控球告警联动抓拍，应符合以下要求：
a）应具备视频终端设定功能，设定内容包括设置视频终端定位信息、视频终端云台预置位初使化信息；
b）应具备定位类告警联动视频功能，对告警人员进行视频追踪及抓拍；
c）应具备人员登高与视频联动功能，支持对登高人员的视频追踪及视频画面自动缩放功能；
d）应具备对现场云台、布控球等监控视频终端的遥控、遥调功能，支持现场违章的视频追踪及抓拍。

10.1.8 支撑目标与行为智能识别分析

应具备基于视觉的目标检测与行为感知分析图像智能识别功能，可对现场传感数据及视频进行实时分析，应符合以下要求：
a）应具备通过指令对违章识别功能进行启用/停用的控制功能，支持对每个规则中采用的违章、告警条件进行配置；
b）应具备算法运行状态监测功能，支持运行状态异常算法的自动重启；
c）应具备远程更新算法模型功能；
d）应具备识别类别扩容功能。

10.2数据可视化

10.2.1 智能服务数据可视化

应具备智能服务侧数据可视化展示功能，应符合以下要求：
a）应具备全国/全省现智能终端在线和离线数量的统计功能；
b）应具备全国/全省智能终端绑定计划列表展示；
c）应具备全国/全省智能终端告警信息实时展示；
d）应具备按作业计划类型统计智能终端绑定的计划数量的功能；
e）应具备智能终端告警数据按告警级别统计告警数量的功能；
f）应具备按地图区域展示智能终端数量和计划数量的功能。

10.2.2 现场管控终端数据可视化

应具备现场管控终端数据可视化展示功能，应符合以下要求：
a）应具备现场视频终端画面实时预览功能；
b）应具备现场告警抓拍图片的预览功能；
c）应具备现场告警录像与录像回放功能，告警录像时长应不低于 7 秒；
d）应具备在手持终端上预览作业区、危险区和标识区等电子围栏的区域位置的功能；
e）应具备人员定位实时可视化监控功能；
f）应具备作业计划信息数据展示功能；
g）应具备作业阶段进度实时展示功能。

11 数据归档共享

11.1样本数据共享

11.1.1 违章数据来源

违章作业视频或图片应来自实际作业数据，在作业人员违规作业时，由布控球抓拍并分析违章，确认违章后才认为是样本数据。

11. 1. 2 违章数据处理

在上报违章数据时，应先将将样本上传至 OSS 存储以完成共享，结构化数据采用 JSON 格式，采用 MQ 的方式将数据推送至云端平台，后续由云端平台相关人员确认为违章数据或者为误报数据，确认违章时收集至正样本库，误报数据则收集至负样本库。

11.2AI 模型共享

11. 2. 1 模型上传

模型应支持容器化部署，可将模型打成 Docker 镜像包，上传至人工智能平台，由相关人员完成部署。

11. 2. 2 模型使用

模型应对外提供 HTTP 协议的接口，模型返回值应满足规范的 JSON 格式，并提供配套的接口说明文档以便使用。

12 数据销毁

应符合 GB/T 22239—2019 中数据备份恢复要求，具备对现场作业视频、违章图像等业务数据，以及云侧智能服务、边侧现场管控终端系统运行日志管理功能。

12.1智能服务数据销毁

智能服务系统日志数据销毁：

a） 登录日志：应至少留存 6 个月，应支持每天自动上传备份，对于超过 6 个月的日志数据，应及时进行删除处理；

b） 操作日志：应至少留存 6 个月，应支持每天自动上传备份，对于超过 6 个月的日志数据，应及时进行删除处理；

c） 异常日志：应至少留存 6 个月，应支持每天自动上传备份，对于超过 6 个月的日志数据，应及时进行删除处理；

d） 告警日志：应至少留存 6 个月，应支持每天自动上传备份，对于超过 6 个月的日志数据，应及时进行删除处理；

e） 监控日志：应至少留存 6 个月，应支持每天自动上传备份，对于超过 6 个月的日志数据，应及时进行删除处理；

f） 接口日志：应至少留存 6 个月，应支持每天自动上传备份，对于超过 6 个月的日志数据，应及时进行删除处理。

12.2现场管控终端数据销毁

12. 2. 1 现场管控终端系统日志数据销毁

a） 登录日志：应至少留存 6 个月，应支持每天自动上传备份，对于超过 6 个月的日志数据，应及时进行删除处理；

b） 操作日志：应至少留存 6 个月，应支持每天自动上传备份，对于超过 6 个月的日志数据，应及时进行删除处理；

c） 异常日志：应至少留存 6 个月，应支持每天自动上传备份，对于超过 6 个月的日志数据，应及时进行删除处理；

d） 告警日志：应至少留存 6 个月，应支持每天自动上传备份，对于超过 6 个月的日志数据，应及时进行删除处理；
e） 监控日志：应至少留存 6 个月，应支持每天自动上传备份，对于超过 6 个月的日志数据，应及时进行删除处理；
f） 接口日志：应至少留存 6 个月，应支持每天自动上传备份，对于超过 6 个月的日志数据，应及时进行删除处理。

12.2.2 现场作业视频数据销毁

a） 应将现场管控终端视频录像数据至少留存 12 个小时；
b） 应将超过 12 个小时的现场管控终端视频录像删除。

12.2.3 违章识别数据销毁

a） 告警视频：应在告警时将告警视频上传至云端，现场管控终端应在作业结束后删除告警视频；
b） 违章图像：应在告警时将违章图像上传至云端，现场管控终端应在作业结束后删除违章图像。

13 数据安全和隐私保护

13.1云边端数据传输安全防护

a） 应具备基于角色的访问控制，确保每个用户只能访问其权限范围内的数据的功能；
b） 应使用传输层安全加密协议对消息队列遥测传输数据进行加密传输功能；
c） 应对敏感数据通过国密 SM4 加密存储，应使用国密 SM4 对存储数据进行加密，并保护加密密钥的安全功能；
d） 应具备前后端加密传输功能，后端使用国密 SM4 加密，传输时加密为国密 SM2 加密推送，并在前端进行国密 SM2 解密。确保数据端到端之间在整个传输过程中都保持加密状态的功能；
e） 应具备对系统安全规则的配置，可配置登录 IP 白名单及登录时间段以及限制对云边端系统的访问功能；
f） 应避免使用不安全的协议（如 FTP）进行数据传输，应采用对象存储服务文件传输协议进行文件传输的功能；
g） 应具备 SQL 注入拦截功能，在接收到 SQL 注入的数据请求时，对该请求进行拦截。

13.2智能服务数据防护

智能数据防护应符合 T/CES 133—2022 的规定，应符合以下要求：

a） 应具备基于角色的访问控制，确保每个用户只能访问其权限范围内的数据的功能；
b） 应使用 TLS/SSL 加密协议对 MQTT 数据进行加密传输功能；
c） 应对敏感数据通过国密 4 加密存储，应使用国网 SM4 对存储数据进行加密，并保护加密密钥的安全功能；
d） 应具备前后端加密传输功能，后端使用 SM4 加密，传输时加密为 SM2 加密推送，并在前端进行 SM2 解密。确保数据端到端之间在整个传输过程中都保持加密状态的功能；
e） 应具备对系统安全规则的配置，可配置登录 IP 白名单及登录时间段以及限制对云边端系统的访问功能；
f） 应避免使用不安全的协议（如 FTP）进行数据传输，应采用 OSS 文件传输协议进行文件传输的功能；
g） 应具备 SQL 注入拦截功能，接收到 SQL 注入的数据，对该请求进行拦截。

13.3现场管控终端防护

现场管控终端防护应符合 T/CES 132—2022 的规定，应符合以下要求：

a）在终端与统一视频平台通讯时，应具备通过加密模块配置统一视频平台申请的证书，密钥，私钥进行拨号接入的功能；

b）在终端与省内网平台交互时，应具备通过省内网平台的接入证书和独立的内网拨号程序进行拨号接入的功能；

c）应具备 onvif 协议的身份认证功能，视频设备使用 onvif 协议接入时，需通过 onvif 协议进行身份认证；

d）应使用传输层安全加密协议对消息队列遥测传输数据进行加密传输功能。

团体标准

电力作业现场智能化安全管控系统
第 4 部分：数据管理与分析技术规范

T/CESXXXX—2024

2024 年 5 月第一版

*

北京西城区莲花池东路 102 号天莲大厦 10 层

邮政编码：100055

网址：http://ces.org.cn/html/category/17060132-1.htm

电话：010-6325699063256997