ICS 35.240.50
CCS L 70

T/EJCCSE

团 体 标 准

T/EJCCSE XXX—XXXX

工业用能单位信息中心架构规范

Specification for the Architecture of Information Centers of Industrial
Energy-consuming Units

(征求意见稿)

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX—XX—XX 发布

XXXX—XX—XX 实施

中国商业股份制企业经济联合会 发布

目 次

前言	II
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 总体架构	1
5 硬件架构	2
6 软件架构	3
7 安全架构	3
8 运维架构	4
9 验收与评估	5

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。

本文件由杭州热电集团股份有限公司提出。

本文件由中国商业股份制企业经济联合会归口。

本文件起草单位：杭州热电集团股份有限公司。

本文件主要起草人：

工业用能单位信息中心架构规范

1 范围

本文件规定了工业用能单位信息中心的总体架构、硬件架构、软件架构、安全架构、运维架构、验收与评估。

本文件适用于工业用能单位信息中心架构规范。

2 规范性引用文件

本文件没有规范性引用文件。

3 术语和定义

下列术语和定义适用于本文件。

3.1

信息中心 information center

集中处理、存储和管理工业用能单位能源相关数据及业务信息的场所。

3.2

能源数据采集终端 energy data acquisition terminal

安装在工业生产现场，用于采集各类能源消耗数据（如电力、水、气等）的设备，具备数据预处理和传输功能。

3.3

数据总线 data bus

在信息中心内部，用于连接不同硬件设备和软件模块，实现数据高速传输和共享的通信通道。

4 总体架构

4.1 架构模型

工业用能单位信息中心采用分层分布式架构，自下而上依次为感知层、传输层、数据层、应用层和展示层，各层之间通过标准接口和通信协议进行数据交互。工业用能单位信息中心各企业与总部之间采用星型结构，信息中心建设于总部。

4.2 架构原则

4.2.1 开放性

采用开放的技术标准和通信协议，便于与现有系统集成和未来系统扩展。

4.2.2 可靠性

具备冗余设计和容错机制，确保系统在各种工况下稳定运行，数据不丢失。

4.2.3 可扩展性

架构设计应充分考虑业务增长和技术发展，能够方便地进行硬件设备扩充和软件功能升级。

4.2.4 安全性

遵循信息安全相关标准，采取多重安全防护措施，保障能源数据的机密性、完整性和可用性。

4.2.5 冗余性

架构设计应考虑设备冗余、功能冗余、性能冗余，保证信息中心可满足实际生产需要。

5 硬件架构

5.1 能源数据采集终端

5.1.1 选型要求

根据不同能源类型和采集环境，选用高精度、高可靠性的采集终端，如智能电表、超声波水表、气体流量计等。采集终端应具备抗干扰能力和防护等级，满足工业现场恶劣环境要求。

5.1.2 功能要求

具备实时数据采集、数据缓存、数据预处理（如滤波、校准）和数据传输功能，支持多种通信接口（如 RS485、Modbus TCP、LoRa 等）与传输层设备连接，至少支持三种以上协议，协议标准为公版。

5.2 数据传输设备

5.2.1 有线传输

采用光纤或工业以太网作为主要有线传输介质，构建高速、稳定的内部网络。在数据中心核心区域，应采用冗余链路设计，确保网络通信的可靠性。

5.2.2 无线传输

对于布线困难或移动性要求较高的场景，可选用 Wi-Fi、4G/5G、LoRa 等无线传输技术。无线传输设备应具备良好的抗干扰性能和安全加密机制。

5.2.3 传输安全

各企业与总部之间的传输需采用专线、SDWAN等手段，确保传输安全。

5.3 服务器与存储设备

5.3.1 服务器

根据数据处理和业务应用需求，选用高性能服务器，如机架式服务器或刀片服务器。服务器应具备多核心处理器、大容量内存和高速 I/O 接口，支持虚拟化技术，提高硬件资源利用率。

5.3.2 存储设备

采用磁盘阵列（RAID）技术构建数据存储系统，根据数据重要性和访问频率，选择合适的 RAID 级别（如 RAID 1、RAID 5、RAID 10 等）。同时，配备磁带库或网络附加存储（NAS）设备，用于数据备份和长期存储。

5.3.3 整体技术

应采用超融合等技术将物理服务器、物理存储设备整合成资源池，以方便业务系统调用。

5.4 网络设备

5.4.1 交换机

选用企业级交换机，具备高带宽、低延迟、端口扩展能力和 VLAN 划分功能，满足信息中心内部网络数据交换需求。在核心层和汇聚层，应采用冗余交换机配置，提高网络可靠性。

5.4.2 路由器

用于连接信息中心内部网络与外部网络，实现数据的路由转发。路由器应具备强大的路由处理能力和安全防护功能，支持多种路由协议（如 OSPF、BGP 等）。

5.4.3 边界防护设备

用于信息中心内部各区域、企业与集团之间的安全防护。

6 软件架构

6.1 操作系统

6.1.1 服务器操作系统

必要时应选择信创类产品，可选用 Windows Server、Linux 等主流操作系统，根据业务需求进行定制化配置。操作系统应定期更新安全补丁，确保系统安全稳定运行。

6.1.2 客户端操作系统

必要时应选择信创类产品，监控终端和操作终端可采用 Windows、MacOS 或 Linux 操作系统，安装必要的安全防护软件，保障用户终端安全。

6.2 数据库管理系统

6.2.1 选型

根据能源数据特点和业务需求，选择关系型数据库（如 MySQL、Oracle）或非关系型数据库（如 MongoDB、InfluxDB）。关系型数据库适用于结构化数据存储和复杂查询，非关系型数据库适用于海量时序数据存储和快速读写，选型时应考虑信创类产品。

6.2.2 功能要求

具备数据存储、查询、备份、恢复、优化等功能，支持数据的高并发访问和分布式部署，确保能源数据的高效管理和利用。

6.3 能源管理软件平台

6.3.1 数据采集与传输模块

负责与能源数据采集终端通信，实现数据的实时采集和传输，并对采集数据进行校验和纠错。

6.3.2 数据处理与分析模块

对采集到的能源数据进行清洗、转换、统计分析，挖掘数据价值，为能源管理决策提供数据支持。支持数据可视化展示，如趋势图、柱状图、饼图等。

6.3.3 设备管理模块

对信息中心硬件设备和软件系统进行统一管理，包括设备状态监测、故障报警、维护计划制定等功能，保障系统正常运行。

6.3.4 用户管理与权限模块

实现用户注册、登录、权限分配等功能，根据用户角色和职责，赋予不同的数据访问和操作权限，确保系统安全。应建立统一身份认证系统，规范系统之间的权限分配。

7 安全架构

7.1 物理安全

7.1.1 机房选址与建设

信息中心机房应选择在地质稳定、环境适宜、远离干扰源的位置。机房建筑应具备防火、防水、防盗、防电磁干扰等功能，采用防火材料装修，安装防水地漏和漏水检测系统，设置门禁系统和监控摄像头。

7.1.2 设备防护

服务器、存储设备、网络设备等硬件设备应安装在标准机柜内，采取加固措施，防止设备晃动和损坏。配备不间断电源（UPS），确保设备在停电情况下正常运行。

7.1.3 机房评级

总部机房应获得国家B级机房评测

7.2 网络安全

7.2.1 网络隔离

采用防火墙、网闸等设备，实现信息中心内部网络与外部网络的隔离，以及内部不同安全区域之间的隔离。设置严格的访问控制策略，限制非法网络访问。

7.2.2 入侵检测与防御

部署入侵检测系统（IDS）和入侵防御系统（IPS），实时监测网络流量，及时发现和阻断网络攻击行为，如 DDoS 攻击、SQL 注入攻击等。

7.2.3 安全审计

建立网络安全审计系统，对网络访问行为进行记录和审计，便于事后追溯和安全事件分析。

7.2.4 等保

因满足并获得等保二级及上，重点单位应在三级

7.3 数据安全

7.3.1 数据加密

对能源数据在传输和存储过程中进行加密处理，采用 SSL/TLS 加密协议保障数据传输安全，采用 AES、RSA 等加密算法对存储数据进行加密，防止数据被窃取和篡改。

7.3.2 数据备份与恢复

制定完善的数据备份策略，定期对重要能源数据进行全量备份和增量备份。备份数据应存储在异地灾备中心，确保数据的安全性和可用性。定期进行数据恢复演练，验证备份数据的完整性和可恢复性。数据备份周期应为一日一备，系统备份应为每次更新前，平台备份应为一日一备。

8 运维架构

8.1 人员组织与职责

8.1.1 系统管理员

负责信息中心硬件设备和软件系统的日常管理和维护，包括设备巡检、故障处理、软件升级等工作。

8.1.2 数据管理员

负责能源数据的管理和维护，包括数据采集、存储、备份、恢复、分析等工作，确保数据的准确性和完整性。

8.1.3 安全管理员

负责信息中心的安全管理工作，包括安全策略制定、安全设备配置、安全事件处理等工作，保障系统安全稳定运行。

8.2 运维流程与制度

8.2.1 日常巡检制度

制定详细的日常巡检计划，对硬件设备、软件系统、网络设施等进行定期巡检，记录巡检结果，及时发现和处理潜在问题。

8.2.2 故障处理流程

建立完善的故障处理流程，明确故障报告、故障诊断、故障修复等环节的责任人和时间节点，确保故障得到及时有效处理。

8.2.3 应急响应预案

制定信息中心应急响应预案，针对火灾、地震、网络攻击、数据丢失等突发事件，明确应急处置措施和流程，定期进行应急演练，提高应急响应能力。

9 验收与评估

9.1 验收标准

9.1.1 硬件验收

依据硬件设备采购合同和相关技术标准，对能源数据采集终端、服务器、存储设备、网络设备等硬件设备的规格、性能、安装质量等进行验收。

9.1.2 软件验收

根据软件功能需求规格说明书，对操作系统、数据库管理系统、能源管理软件平台等软件系统的功能、性能、稳定性、安全性等进行测试和验收。

9.1.3 安全验收

按照信息安全相关标准和规范，对信息中心的物理安全、网络安全、数据安全等方面进行检查和评估，确保安全防护措施符合要求。

9.2 运行评估

9.2.1 定期评估

信息中心投入运行后，定期（如每季度或每年）对其运行效果进行评估，包括能源管理效率、数据准确性、系统稳定性、安全性等方面。

9.2.2 改进措施

根据运行评估结果，分析存在的问题和不足，制定针对性的改进措施，不断优化信息中心架构和性能，提高能源管理水平。