

T/EJCCCSE

团 体 标 准

T/EJCCCSE XXX—XXXX

热网监控系统技术规范

Technical Specifications for Heat Network Monitoring System

（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 系统架构 1

5 功能要求 2

6 安全要求 4

7 维护与升级 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：

热网监控系统技术规范

1 范围

本文件规定了热网监控系统的系统架构、功能要求、安全要求、维护与升级。
本文件适用于热网监控系统技术规范。

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

热网监控系统 **heat network monitoring system**
实现对热网运行参数实时监测、控制和管理的自动化系统。

4 系统架构

4.1 总体架构

4.1.1 感知层

由各类传感器、智能仪表等设备组成，负责采集热网运行的实时数据，如温度、压力、流量、热量等，并将数据上传至传输层。

4.1.2 传输层

采用有线和无线相结合的传输方式，将感知层采集的数据传输至数据层。有线传输可选用光纤、以太网等，无线传输可采用 4G/5G、LoRa、Wi-Fi 等技术。

4.1.3 数据层

由数据库服务器、数据存储设备等组成，负责存储和管理热网运行的实时数据和历史数据。数据库应具备高可靠性、高可用性和高性能，支持数据的快速查询和分析。

4.1.4 应用层

由监控软件、数据分析软件、调度决策软件等组成，为用户提供热网监控、数据分析、调度决策等功能。应用层软件应具备友好的用户界面，操作简单、方便。

4.2 硬件架构

4.2.1 传感器

根据热网监测需求，选用高精度、高可靠性的温度传感器、压力传感器、流量传感器、热量表等设备。传感器应具备良好的抗干扰能力和防护性能，满足现场安装环境要求。

4.2.2 数据采集终端

负责采集传感器数据，并对数据进行预处理和缓存。数据采集终端应具备通信接口，支持与传输层设备进行数据传输。

4.2.3 传输设备

包括交换机、路由器、无线接入点等设备，负责构建热网监控系统的通信网络，实现数据的可靠传输。

4.2.4 服务器

选用高性能的服务器，用于运行数据库管理系统、监控软件和数据分析软件等。服务器应具备冗余电源、冗余硬盘等配置，确保系统的高可靠性。

4.2.5 监控终端

包括计算机、工业平板电脑等设备，为用户提供热网监控和操作界面。监控终端应具备良好的显示性能和操作性能，方便用户使用。

4.3 软件架构

4.3.1 操作系统

服务器操作系统可选用 Windows Server、Linux 等主流操作系统，监控终端操作系统可选用 Windows、Linux 等。操作系统应具备良好的稳定性和安全性，定期进行更新和维护。

4.3.2 数据库管理系统

选用关系型数据库管理系统，如 Oracle、MySQL 等，用于存储和管理热网运行数据。数据库管理系统应具备数据备份、恢复、优化等功能，确保数据的安全和高效访问。

4.3.3 监控软件

实现对热网运行状态的实时监测、报警处理、远程控制等功能。监控软件应具备友好的用户界面，支持图形化展示、数据查询、报表生成等功能。

4.3.4 数据分析软件

对热网运行历史数据进行分析，挖掘数据价值，为热网优化调度、故障预测等提供决策支持。数据分析软件应具备数据挖掘、统计分析、机器学习等功能。

4.3.5 通信协议

热网监控系统内部各设备之间应采用统一的通信协议，如 Modbus、OPC UA 等，确保设备之间的互联互通和数据共享。

5 功能要求

5.1 数据采集功能

5.1.1 实时采集

系统应能够实时采集热网各监测点的温度、压力、流量、热量等参数，采集周期可根据实际需求设置，一般不超过 1 min。

5.1.2 数据校验

对采集到的数据进行校验，剔除异常数据，确保数据的准确性和可靠性。数据校验方法包括数据范围校验、数据变化率校验、数据相关性校验等。

5.1.3 数据缓存

在数据传输过程中，如遇网络故障或其他异常情况，数据采集终端应具备数据缓存功能，将采集到的数据临时存储在本地，待网络恢复正常后，自动将缓存数据上传至服务器。

5.1.4 采集规范

5.1.4.1 应做好物理访问控制。

5.1.4.2 应具备日志功能，应存储不少于七天的完整日志。

5.1.4.3 采集数据应至少包含：发射时间、计量数据、校验码、设备实时状态等数据。

5.2 数据传输功能

5.2.1 可靠传输

传输层应确保数据传输的可靠性，采用冗余通信链路、数据重传等技术，保证数据传输的完整性和准确性。数据传输误码率应不超过 10^{-6} 。

5.2.2 传输速率

根据热网数据量和实时性要求，合理选择传输设备和传输技术，确保数据传输速率满足系统需求。一般情况下，实时数据传输延迟应不超过 5 s。

5.2.3 通信协议转换

对于不同通信协议的设备，系统应具备通信协议转换功能，实现设备之间的数据互联互通。

5.3 数据存储功能

5.3.1 历史数据存储

系统应能够存储热网运行的历史数据，存储时间不少于 5 年。历史数据应按照时间顺序进行存储，方便查询和分析。

5.3.2 数据备份与恢复

定期对热网运行数据进行备份，备份数据应存储在异地存储设备中，以防止数据丢失。当系统发生故障或数据丢失时，应能够快速恢复数据。

5.3.3 数据存储优化

采用数据压缩、数据分区等技术，对热网运行数据进行存储优化，提高数据存储效率和查询速度。

5.4 监控功能

5.4.1 实时监控

通过监控软件，实时展示热网的运行状态，包括各监测点的参数、管网拓扑结构、设备运行状态等。监控界面应采用图形化展示方式，直观、清晰。

5.4.2 报警功能

当热网运行参数超过设定的阈值或设备发生故障时，系统应及时发出报警信息，通知相关人员进行处理。报警方式包括声音报警、短信报警、邮件报警等。

5.4.3 远程控制

系统应具备远程控制功能，可对热网中的调节阀、水泵等设备进行远程操作，实现热网的优化调度和节能运行。远程控制操作应具备权限管理和操作记录功能，确保操作的安全性和可追溯性。

5.4.4 GIS 地图功能

系统应具备 GIS 地图功能，将热用户在 GIS 地图中予以展示，并在 GIS 地图上关联用户信息、设备信息、生产信息等数据。

5.5 数据分析功能

5.5.1 数据统计分析

对热网运行历史数据进行统计分析，生成各类报表和图表，如日报表、月报表、年报表、能耗分析图表、负荷曲线等，为热网运行管理提供数据支持。

5.5.2 能耗分析

分析热网的能耗情况，找出能耗高的环节和原因，提出节能改进措施。能耗分析应包括能源消耗统计、能源效率分析、节能潜力评估等内容。

5.5.3 故障分析

对热网运行过程中发生的故障进行分析，找出故障原因和规律，提出故障预防措施。故障分析应包括故障统计、故障原因分析、故障预测等内容。

5.5.4 趋势分析

根据热网运行历史数据，预测热网未来的运行趋势，如负荷变化趋势、能耗变化趋势等，为热网的规划和调度提供决策依据。

5.6 热用户功能

5.6.1 时数据

针对不同热用户显示该热用户当前生产情况。

5.6.2 历史数据

针对不同热用户显示该热用户历史生产情况。

5.6.3 支付管理

针对不同热用户显示该热用户资金使用情况，应支持多种线上支付接口。

5.6.4 设备管理

热用户查看与自己相关的管网设备。

5.7 系统管理功能

5.7.1 用户管理

对热网监控系统的用户进行管理，包括用户注册、登录、权限分配等功能。用户权限应分为管理员、操作员、普通用户等不同级别，不同级别用户具有不同的操作权限。

5.7.2 设备管理

对热网监控系统中的硬件设备和软件系统进行管理，包括设备台账管理、设备状态监测、设备维护计划制定等功能。设备管理应实现设备的全生命周期管理，提高设备的可靠性和使用寿命。

5.7.3 系统配置管理

对热网监控系统的参数进行配置和管理，包括监测点配置、报警阈值设置、通信参数设置等功能。系统配置管理应具备参数备份和恢复功能，确保系统配置的安全性和稳定性。

5.7.4 可扩展性

系统应设置独立接口，用于系统数据与其它系统对接或转存。

5.7.5 日志审计

系统应根据接收时间、接收内容、校验码等内容保存原始日志。

6 安全要求

6.1 数据安全

6.1.1 数据加密

对热网运行数据进行加密传输和存储，防止数据被窃取和篡改。数据加密算法应采用国际标准的加密算法，如 AES、RSA 等。

6.1.2 数据备份与恢复

定期对热网运行数据进行备份，备份数据应存储在异地存储设备中。当系统发生故障或数据丢失时，应能够快速恢复数据。应采用一日一备的备份策略。

6.1.3 数据访问控制

对热网运行数据的访问进行控制，只有授权用户才能访问和操作数据。数据访问控制应采用用户身份认证、权限管理等技术。

6.2 网络安全

6.2.1 网络隔离

将热网监控系统与外部网络进行隔离，防止外部网络对系统的攻击和入侵。网络隔离可采用防火墙、网闸等设备。

6.2.2 入侵检测与防范

部署入侵检测系统（IDS）和入侵防范系统（IPS），实时监测网络流量，及时发现和防范网络攻击行为。

6.2.3 漏洞管理

定期对热网监控系统的软件和硬件进行漏洞扫描，及时发现和修复系统漏洞。漏洞管理应建立漏洞数据库，对漏洞进行跟踪和管理。

6.3 物理安全

6.3.1 设备防护

对热网监控系统的硬件设备进行防护，防止设备被盗、损坏和遭受自然灾害。设备防护应采取安装防盗报警装置、配备 UPS 电源、设置防雷接地等措施。

6.3.2 机房安全

对热网监控系统的机房进行安全管理，包括机房门禁管理、机房环境监测、机房消防等。机房安全应符合相关标准和规范的要求。

6.3.3 操作站安全

热网监控系统系统操作站应具备专人专机专用，分隔权限，并与服务器之间做好防护措施。

7 维护与升级

7.1 维护要求

7.1.1 日常维护

建立热网监控系统的日常维护制度，定期对系统进行巡检和维护，检查系统的运行状态和设备的工作情况。日常维护应包括设备清洁、设备校准、数据备份、软件更新等内容。

7.1.2 故障维修

当热网监控系统发生故障时，应及时进行故障诊断和维修，恢复系统的正常运行。故障维修应建立故障报告和维修记录制度，对故障原因和维修情况进行详细记录。

7.1.3 维护培训

对热网监控系统的维护人员进行培训，提高维护人员的技术水平和业务能力。维护培训应包括系统原理、设备操作、故障诊断、维修技术等内容。

7.2 升级要求

7.2.1 软件升级

根据热网监控系统的发展需求和技术进步，及时对系统软件进行升级，增加新的功能和优化现有功能。软件升级应经过严格的测试和验证，确保升级后的系统稳定、可靠。

7.2.2 硬件升级

当热网监控系统的硬件设备性能不能满足系统需求时，应及时对硬件设备进行升级，提高系统的处理能力和运行效率。硬件升级应根据系统的实际情况进行合理规划和设计，确保硬件设备的兼容性和可靠性。

7.2.3 升级管理

建立热网监控系统的升级管理制度，对系统升级进行统一规划、管理和实施。升级管理应包括升级需求分析、升级方案制定、升级测试、升级实施和升级后评估等内容。
