ICS 33.040.40
CCS L 78

团　　体　　标　　准

T/EJCCCSE XXXX—XXXX

网络与负载的边缘网关集群算力调度系统

Edge gateway cluster computing power scheduling system for network and load

（征求意见稿）

2024－XX－XX 发布　　2024－XX－XX 实施

中国商业股份制企业经济联合会　　发 布

目　　次

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。

本文件由浙江宇丰信息技术有限公司提出。

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：浙江宇丰信息技术有限公司、×××。

本文件主要起草人：×××。

网络与负载的边缘网关集群算力调度系统

1 范围

本文件规定了网络与负载的边缘网关集群算力调度系统的一般要求、系统架构、功能要求、性能要求、运行和维护管理、安全管理。

本文件适用于网络与负载的边缘网关集群算力调度系统。

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 25000.51 系统与软件工程 系统与软件质量要求和评价(SQuaRE) 第51部分:就绪可用软件产品(RUSP)的质量要求和测试细则

GB/T 28827.1 信息技术服务 运行维护 第1部分:通用要求

GB/T 28827.2 信息技术服务 运行维护 第2部分:交付规范

GB/T 28827.3 信息技术服务 运行维护 第3部分:应急响应规范

GB/T 35319 物联网 系统接口要求

GB/T 41479 信息安全技术 网络数据处理安全要求

GB/T 41782.1 物联网 系统互操作性 第1部分:框架

GB/T 41782.2 物联网 系统互操作性 第2部分:网络连通性

GM/T 0054 信息系统密码应用基本要求

JB/T 14347.2 工业机械电气设备及系统数控系统功能测试规范 第2部分:基本功能

3 术语和定义

本文件没有需要界定的术语和定义。

4 一般要求

4.1 系统的设计应符合 JB/T 14347.2 的相关规定。

4.2 系统的用户文档应符合 GB/T 25000.51 的规定。

4.3 系统应具有良好的扩展性，包括但不限于系统功能、数据接口、系统处理能力的可扩展，并支持定制功能开发。

4.4 系统的接口应符合 GB/T 35319 的规定。

4.5 系统的系统互操作性应符合 GB/T 41782.1、GB/T 41782.2 的规定。

5 系统架构

系统架构如图 1 所示。

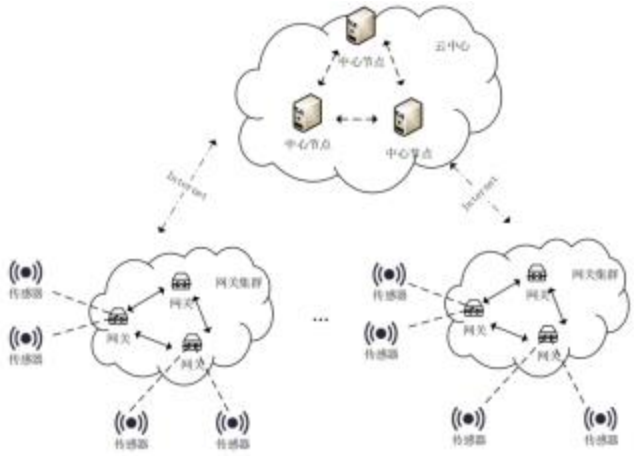

图1　系统架构图

6　功能要求

系统应具有以下功能：

a)　可通过部署在工作区域内的工业网关获取工业数据；
b)　可将同一工作区域内的多台工业网关组成网关集群；
c)　可采用 Raft 算法使网关集群内的各个工业网关之间的工业数据进行同步；
d)　计算在不同网关集群内的工业网关节点上处理所述工业数据所需的成本开销和/或在云端节点上处理所述工业数据所需的成本开销；
e)　基于所述成本开销通过 Qlearning 强化算法对不同网关集群内的工业网关节点和/或云端节点上的计算任务进行分配。

7　性能要求

7.1　系统运行

应支持 7 d×24 h 不间断运行。

7.2　响应时间

应不大于 2 s。

7.3　易用性

7.3.1　应用户界面友好，操作简单，易于掌握。
7.3.2　应提供用户手册或操作规程。

7.4　兼容性

应兼容主流操作系统，数据接口基于标准的互联网协议。

7.5　数据储存和备份

7.5.1　数据在线存储时间应不少于 183 d。
7.5.2　应建立数据备份机制，每月对数据进行全量备份，每周对数据进行增量备份。
7.5.3　应支持备份数据的下载。

8　运行和维护管理

8.1　基本要求

8.1.1 系统的运行和维护管理应由系统管理单位承担,配置专职安全管理人员并明确各系统角色权限、责任和风险。
8.1.2 系统运行操作人员应具备熟练操作系统的能力，并经考核合格。
8.1.3 技术运维人员应有系统运维的能力，并按本文件的规定对系统进行日常检查和维护。

8.2 运行管理

8.2.1 网络运行和安全

8.2.1.1 管理单位应对正常运行中的系统进行在线监测，当出现数据中断或有差异时应立即处理。
8.2.1.2 系统出现故障信号时，维护人员应迅速查明原因，修复故障。
8.2.1.3 系统管理人员应定期对网络系统进行查询、监测，并及时对故障进行有效地隔离、排除和恢复。
8.2.1.4 系统应采用通信协议隔离技术，保障信息传输的安全。
8.2.1.5 系统应有攻击防御与溯源安全措施。

8.2.2 数据库安全

8.2.2.1 系统数据库应包括数据存储子系统、数据备份子系统。
8.2.2.2 系统数据库数据备份子系统应透明、自动实现，并提供管理功能。
8.2.2.3 系统数据库数据格式与接入系统数据格式应一致。

8.2.3 应用安全

8.2.3.1 对用户访问网络资源的权限应有认证和控制。
8.2.3.2 系统管理人员应监督数据库使用权限、用户密码使用情况，用户应定期更换密码。

8.2.4 终端安全

8.2.4.1 应由专业的技术人员负责对系统的软件、设备、设施的安装、调试、排除故障，其他单位和个人不应自行拆卸或安装任何软、硬件设施。
8.2.4.2 系统终端应设置防火墙，安装防病毒软件。

8.3 运维安全管理

8.3.1 运行维护基本要求应符合 GB/T 28827.1 的要求，运行维护的交付应符合 GB/T 28827.2 的要求，运行维护的应急响应符合 GB/T 28827.3 的要求。
8.3.2 应建立完善的运维保障机制，配备专门的运维人员。
8.3.3 应根据智慧城建需求和系统安全分析确定系统的访问控制策略。
8.3.4 应定期进行漏洞扫描，对发现的系统安全漏洞及时进行修补。
8.3.5 应安装系统的最新补丁程序，在安装系统补丁前，应先在测试环境中测试通过，并对重要数据进行备份后，方可实施系统补丁程序的安装。
8.3.6 应建立系统安全管理制度，对系统安全策略、安全配置、日志管理等方面作出具体规定。
8.3.7 应依据操作手册对系统进行维护，详细记录操作日志，包括重要运行维护记录、智慧城建项目的设置等内容，不准许进行未经授权的操作；应定期对运行日志进行分析，及时发现异常行为。
8.3.8 应建立健全的数据对接维护机制，设置专人负责数据对接运维工作，并定期整理信息。
8.3.9 运维人员账号应实行权限管理，定期修改账号密码。

8.4 运维制度

8.4.1 应建立运维管理的工作机制，制定以下制度：
a) 日常运维管理制度，包括运维操作规程、人员日常操作管理等；
b) 运维过程管理制度，包括运维各个环节管理、操作流程等。
8.4.2 应建立运维管理制度制定、发布、维护和更新的机制，定期修订和完善运维管理制度。

8.5 应急处置

8.5.1 应制定系统运行异常应急恢复方案，定期组织演练。应急恢复方案应包括网络、硬件设备、软件系统等异常情况的处置方案和应急操作手册，确保系统安全高效运行。
8.5.2 可聘请专业人员定期对系统进行巡检，发现问题应及时处理。

9 安全管理

9.1 应保证接入系统的设备、系统、用户以及数据传输的安全。
9.2 应建立系统安全响应和反馈机制，及时受理安全性相关的提示、咨询和建议等。
9.3 系统密码应用应符合 GM/T 0054 的要求。
9.4 系统网络安全等级保护应符合 GB/T 22239—2019 中第二级安全要求。
9.5 系统数据处理应符合 GB/T 41479 的要求。