ICS 35.240.60
CCS L 70

T/GXAS

团　　体　　标　　准

T/GXAS 1406—2026

高速公路收费站机房网络智能化运维管理规范

Specification for operation and maintenance management of network Intelligent in expressway toll station data centers

2026－08－14 发布　　2026－08－20 实施

广西标准化协会　　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　缩略语 1
5　基本要求 2
5.1　组织 2
5.2　基础设施与环境 2
5.3　管理要求 2
6　智能化巡视检查 2
6.1　管理对象与监控 2
6.2　智能化巡检 2
6.3　知识库 3
6.4　网络性能 4
6.5　人工巡检 4
7　维护更新 4
7.1　故障处理 4
7.2　设备与系统维护 4
7.3　变更与升级 5
8　数据管理 5
8.1　数据分类与留存 5
8.2　数据质量控制 5
8.3　灾备管理 5
8.4　数据安全管理 6
9　网络安全管理 6
9.1　边界防护 6
9.2　终端安全 7
9.3　接入管控 7
9.4　漏洞与补丁管理 7
9.5　网络安全等级保护 7
9.6　智能化安全要求 7
参考文献 8

前　言

本文件参照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。

本文件由广西网络安全和信息化联合会提出、归口并宣贯。

本文件起草单位：广西福玉高速公路有限公司、广西智投机电工程有限公司、广西交通投资集团梧州高速公路运营有限公司、广西网络安全和信息化联合会、广西智能交通科技有限公司。

本文件主要起草人：秦曙光、覃瑞宏、刘聪、李诗荣、聂林焕、刘耀喜、张龙生、李莉莉、邵先涛、覃信满、朱帅学、奉佳、蔡俊、尹哲明、覃贵耀、吴玮、石方楠、陈佳、李俊辉、江静鹏、韦芳圻、蔡凌燕。

高速公路收费站机房网络智能化运维管理规范

1 范围

本文件界定了高速公路收费站机房网络智能化运维管理涉及的术语和定义以及缩略语，规定了高速公路收费站机房网络智能化运维管理的基本要求、智能化巡视检查、维护更新、数据管理、网络安全管理的要求。

本文件适用于高速公路收费站机房网络智能化运维管理。

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 2887 计算机场地通用规范

GB/T 20281 信息安全技术 防火墙安全技术要求和测试评价方法

GB/T 22239 信息安全技术 网络安全等级保护基本要求

GB/T 25070 信息安全技术 网络安全等级保护安全设计技术要求

GB 50174 数据中心设计规范

JTG 6310 收费公路联网收费技术标准

JTG/T 6311 收费公路联网收费系统检测规范

YD/T 4242 电信网和互联网数据安全日志审计指南

3 术语和定义

下列术语和定义适用于本文件。

3.1

智能化运维管理 intelligent operation and maintenance management

依托物联网、大数据及人工智能技术，通过自动采集、智能分析与辅助决策等手段，实现高速公路收费站机房网络、设备和业务的主动预警、故障自愈、性能优化及运营数据可视化管理的模式。

3.2

网络性能基线 network performance baseline

基于历史运行数据建立的收费、通讯等核心业务链路正常性能范围，含带宽利用率、延迟、丢包率等，作为异常判定的基准。

4 缩略语

下列缩略语适用于本文件。

ACL：访问控制列表（Access Control List）

CPU：中央处理器（Central Processing Unit）

DDoS：分布式拒绝服务（Distributed Denial of Service）

IDS：入侵检测系统（Intrusion Detection System）

IP：互联网协议地址（Internet Protocol Address）

QoS：服务质量（Quality of Service）

RAID：独立磁盘冗余阵列（Redundant Array of Independent Disks）

UPS：不间断电源（Uninterruptible Power Supply）

URL：统一资源定位符（Uniform Resource Locator）

VLAN：虚拟局域网（Virtual Local Area Network）

VPN：虚拟专用网络（Virtual Private Network）

5 基本要求

5.1 组织

应建立网络运维管理体系，明确组织架构与岗位职责，定期开展技能安全培训及考核。

5.2 基础设施与环境

5.2.1 机房温度、湿度、供配电等物理环境设计应符合 GB 50174 的规定，计算机场地通用要求应符合 GB/T 2887 的规定，网络安全等级保护设计应符合 GB/T 25070 的规定。
5.2.2 应配备火灾自动报警系统，并与气体灭火系统联动。
5.2.3 供配电应采用主备双电源设计，UPS 应采用冗余配置，续航时间≥4 h；机房 UPS 供电切换时间≤10 ms。
5.2.4 线缆、端口、路由标识应规范清晰。
5.2.5 宜采用智能巡检机器人辅助进行设备状态识别和环境监测。
5.2.6 网络架构应采用冗余设计，核心层设备应支持双电源、双引擎，关键链路应具备物理或逻辑上的冗余路径。收费业务链路应配置主备双链路，主链路中断时应在 30 s 内自动切换至备用链路。
5.2.7 应配置智能运维平台、智能化巡检系统。
5.2.8 应建立日志集中分析系统。
5.2.9 应部署机房动力环境监控系统或纳入统一的智能运维平台，系统应具备快速感知能力，故障发现时间≤60 s，告警信息应在 10 s 内通过短信、邮件或移动端应用推送至运维人员。
5.2.10 应建立机房网络运维知识库，具备统一管理、智能检索、自动推送功能。

5.3 管理要求

5.3.1 每半年至少进行 1 次消防演练，灭火系统应每季度巡检、每年至少 1 次全面功能检测，记录存档
5.3.2 机房应实施出入控制，门禁系统应具备权限管理、记录查询功能。
5.3.3 网络拓扑图应动态更新，任何变更后应在 3 个工作日内完成拓扑图及相关配置文件的更新与备份。
5.3.4 应建立网络性能基线管理机制，通过历史数据学习生成核心业务链路的延迟、丢包率、带宽利用率正常波动范围，当实时指标偏离基线时触发预警。

6 智能化巡视检查

6.1 管理对象与监控

6.1.1 运维对象应包括网络设备（核心交换机、汇聚交换机等）、计算存储设备（收费业务服务器、数据库服务器、存储设备等）、安全设备及配套设施等。
6.1.2 应通过运维管理平台对设备运行状态、网络性能及安全事件进行 7×24 h 监控。采用机房动力环境监控系统或纳入统一的智能运维平台对温湿度、漏水、烟雾、供配电、UPS 状态、空调运行等参数进行实时监测和异常告警。
6.1.3 对设备温度、电压等运行参数进行实时监测，温度超 30 ℃、电压偏差±10%时应自动报警。
6.1.4 监控系统应具备告警收敛、告警级别定义和多渠道通知功能。
6.1.5 机房出入口及主要通道应部署视频监控，录像保存时间≥90 d。

6.2 智能化巡检

6.2.1 一般要求

采用智能运维平台对机房网络、服务器、安全、动力环境设备开展全自动巡检作业。

6.2.2 设备状态自动采集

采用智能化巡检系统进行7×24 h自动采集，并满足以下要求：

——采集频率：核心交换机、业务服务器、防火墙等核心设备每 30 s 至少采集 1 次，一般设备每 5 min 至少采集 1 次；

——采集内容：CPU 利用率、内存利用率、磁盘使用率、端口状态、设备温度、电压、端口流量、在线状态、关键进程/服务状态等；

——自动预警：当 CPU 利用率持续＞70%或内存可用＜20%或磁盘使用率＞85%时，系统应自动预警。

6.2.3 网络性能主动探测

应对收费业务链路、稽核链路、视频传输链路、管理链路开展主动式性能探测，并满足以下要求：

——核心链路每 1 min 至少探测 1 次，性能每 5 min 至少采样 1 次；

——监测连通性、延迟、抖动、丢包率；

——当指标偏离动态网络性能基线±50%或丢包率＞0.1%或延迟＞100 ms 时自动告警。

6.2.4 日志智能分析

应采用日志集中分析系统对网络设备、安全设备、服务器、运维操作日志进行统一采集、关联分析、异常识别，并满足以下要求：

——日志采集延迟≤1 min；

——应能自动识别暴力破解、异常登录、未授权配置变更、违规外联、异常流量、账号越权操作等行为；

——发现异常应实时推送告警并形成处置工单。

6.2.5 智能巡检报告

6.2.5.1 智能化巡检系统应每日自动生成巡检报告，报告内容应包括设备健康度统计、性能趋势分析、异常事件汇总、告警处置闭环情况等。

6.2.5.2 报告应支持图表化展示，可按日、周、月自动归档。

6.2.6 高频性能采集

对核心服务器、核心交换机可启用短期高频采集用于性能瓶颈诊断、故障深度分析，并满足以下要求：

——高频采集时长≤10 min，每分钟采集 3～5 次；

——诊断完成后自动恢复常规采集频率，数据应专项归档。

6.3 知识库

6.3.1 知识库内容

知识库应至少包含以下内容：

——智能化巡检标准、巡检项、阈值及判定规则；

——设备典型故障现象、根因、排查步骤及处理方法；

——网络性能基线偏离案例及优化方案；

——配置变更与系统升级操作规范；

——应急处置流程与预案；

——型号参数、硬件规格、厂商维保信息等设备基础信息；

——设备维护保养手册及周期要求；

——常见告警含义及处置指引。

6.3.2 知识库应用

6.3.2.1 应建立知识库与智能巡检系统的联动机制，智能巡检发现异常时，系统应按 6.3.1 的知识库内容自动匹配案例并推送处置建议。

6.3.2.2　故障工单生成时，应自动关联同类历史故障处理方案。
6.3.2.3　巡检任务执行前，应自动展示该点位巡检要点与注意事项。

6.3.3　知识库更新与维护

6.3.3.1　设备配置变更、系统升级后，应在 24 h 内完成知识库相关内容更新。
6.3.3.2　每季度应对知识库进行审核、更新、优化。
6.3.3.3　知识库应支持关键词检索、故障现象检索、设备型号检索。

6.4　网络性能

6.4.1　应每日监测带宽利用率、延迟、丢包率等性能指标是否符合带宽利用率≤70%、网络延迟≤100 ms、丢包率≤0.1%。
6.4.2　收费业务链路的性能应符合 JTG　6310 的规定，并配置主备冗余链路，主链路中断时应在 30 s 内切换。联网收费系统性能的检测应按 JTG/T　6311 的规定执行。
6.4.3　应通过 QoS 策略保障机房内收费业务接入、车牌识别、视频监控等业务的带宽优先级。当机房出口业务带宽利用率≥80%时，应限制办公、互联网访问等非业务流量占比≤10%；当收费、稽核等核心业务接入链路带宽利用率连续 1 h 超过 80%时，应启动性能优化流程，分析流量构成并采取扩容、限流或策略优化等措施。

6.5　人工巡检

6.5.1　节假日前应完成全链路压力测试及设备负载均衡调整。当预测车流量达到平日 2 倍及以上时，应在高峰到来前开展专项巡检。
6.5.2　汛期前 1 周完成机房防水、防雷设施专项巡检。
6.5.3　人工巡检发现异常应及时处理并记录，记录应纳入运维管理平台统一归档。
6.5.4　人工巡检时应同步核对智能化巡检系统及监控平台的告警信息，发现误报、漏报或监测偏差应及时反馈，并优化巡检策略及告警阈值。

7　维护更新

7.1　故障处理

7.1.1　应建立智能化故障处置闭环机制，实现：自动告警→智能研判→工单派发→远程/现场处理→结果验证→复盘归档。
7.1.2　故障按影响范围分为三级：
——一级故障：全站收费业务中断、核心网络瘫痪；
——二级故障：单车道/部分区域业务异常、非核心设备宕机；
——三级故障：单端口异常、性能轻微劣化、一般性告警。
7.1.3　故障响应时间和处置应满足以下要求：
——一级故障：5 min 内响应，30 min 内启动应急处置流程，并根据收费站地理位置明确最长到场时限，4 h 内恢复；
——二级故障：10 min 内响应，2 h 内处置完毕；
——三级故障：24 h 内完成处理。
7.1.4　故障诊断应采用“分层排查法”（数据链路层→网络层→应用层→数据处理），如有必要可通过查询知识库辅助定位原因。
7.1.5　故障修复后应自动验证业务连通性与性能指标，一级故障 7 d 内完成复盘。
7.1.6　应建立告警响应率评价机制，告警响应率应不低于 99%。
注：告警响应率=（规定时间内响应的告警数/告警总数）×100%

7.2　设备与系统维护

维护工作应基于智能运维平台自动生成维护计划，实现预测性维护，并满足以下要求：
——智能运维平台应根据设备运行时长、负载、故障频率、老化程度自动生成维护工单；
——设备除尘、接口清洁、UPS 测试、风扇检测、防雷检测等应由系统自动提醒；

——设备健康度评分低于阈值时，应自动提示提前更换或深度检修；
——网络配置应实行智能备份、自动比对、异常变更告警；
——设备生命周期应由平台自动管理，到期前 6 个月自动提示更新替换；
——设备配置应采用“本地+异地+云端”三重备份，每周全量备份，配置备份文件应加密存储，每年开展 1 次备份恢复测试；
——应每季度对网络设备配置进行审查，清理无效路由、过期 ACL、冗余 VLAN 等冗余配置，配置清理前应备份当前配置，并在业务低峰期执行，执行后应验证业务连通性。

7.3 变更与升级

所有变更与升级应纳入智能化变更管理流程，并满足以下要求：
——变更前应由智能平台进行影响范围分析、风险评估、流量仿真预判；
——变更方案应自动留存，配置应自动备份，回退方案应自动生成；
——变更过程应全程记录，操作日志应不可篡改；
——变更后应由平台自动进行业务测试、性能监测，确认正常后闭环；
——涉及拓扑调整的，应由平台自动更新网络拓扑图并同步归档；
——系统升级应在 00:00～05:00 进行，升级前应备份设备配置、业务数据，备份数据应存储于本地及异地，并测试验证，应安排 2 名及以上运维人员现场操作，1 人执行，1 人监督。

8 数据管理

8.1 数据分类与留存

运维数据分类和存储周期如下：
——设备运行数据：设备温度、电压、CPU 利用率等实时参数，存储周期≥6 个月；
——网络性能数据：带宽利用率、延迟、丢包率等指标，存储周期≥1 年；
——故障处理数据：故障现象、诊断过程、修复措施等记录，存储周期≥3 年；
——安全事件数据：漏洞扫描报告、入侵告警日志、渗透测试结果等，存储周期≥5 年；其中敏感数据应加密存储。

8.2 数据质量控制

8.2.1 采集质量控制

8.2.1.1 温度传感器、网络分析仪等数据采集设备应每年校准，误差范围≤±2%。

注：数据采集：运用自动化工具（如网络爬虫、传感器、日志抓取）或人工录入方式，从收费站机房内的网络设备、计算存储设备、安全设备及配套环境设施中获取原始运行数据、性能指标及状态信息的过程。

8.2.1.2 应采用自动化工具采集数据，采集频率根据数据类型设定：
——CPU、内存、磁盘、温度、电压等设备运行数据每次≤30 s；
——带宽利用率、延迟、丢包率等网络性能数据每次≤5 min。

8.2.2 存储质量控制

8.2.2.1 故障处理数据、安全事件数据等核心数据采用磁盘阵列存储，支持 RAID5 及以上冗余；备份数据采用异地存储，距离宜≥50 km。

8.2.2.2 重要数据应保存 3 份副本、采用 2 种存储介质、其中 1 份存放于异地，每日增量备份，每周全量备份；每月进行 1 次备份恢复测试。

8.2.2.3 每季度检查存储设备的硬盘坏道、存储容量等健康状态，剩余容量低于 20%时及时扩容。

8.3 灾备管理

8.3.1 灾备中心与生产中心的距离宜≥50 km，灾备中心应具备与生产中心同等的存储、计算和网络资源。

8.3.2 应建立灾备切换机制，每年至少开展一次灾备切换演练。演练内容应包含故障模拟、切换执行、业务验证、回退流程，并验证灾备系统的可用性和数据一致性，演练过程应记录并归档。日常运维中，

应每日进行一次数据一致性检查。
8.3.3　灾备系统的备份策略应符合 8.2.2.2 的要求，灾备数据应与生产数据保持同步，同步周期应根据业务重要性设定，核心业务数据同步延迟应≤15 min。
8.3.4　应建立灾备系统巡检机制，每月检查灾备设备运行状态、网络连通性和数据同步情况，发现异常及时处理。

8.4　数据安全管理

8.4.1　访问控制

8.4.1.1　应实施访问控制，采用双因素认证，如“用户名+密码+动态令牌”“用户名+密码+生物特征识别”“用户名+数字证书”等组合方式；密码应长度≥8 位，含大小写字母、数字、特殊符号，密码每 90 d 更换。
8.4.1.2　基于岗位职责设置角色权限，权限变更应经审批，并记录权限变更。
8.4.1.3　远程运维会话超时时间≤30 min，关闭未使用会话；不应共享账号，发现账号异常登录立即锁定。
8.4.1.4　特权账号的使用应经过审批，并记录所有操作。
8.4.1.5　运维终端应安装终端安全管理软件，不应安装非授权应用；通过 USB 端口管控，非授权存储设备不应接入，仅授权特定标签的 U 盘可读取数据。

8.4.2　数据加密

8.4.2.1　数据传输采用 SSL 或 TLS 1.2 及以上协议加密，密钥长度≥2 048 位。
8.4.2.2　设备密码、收费交易日志等敏感数据存储时采用 SM4 国密算法进行加密存储，加密密钥由专人保管，每 6 个月更换。
8.4.2.3　建立密钥生命周期管理机制，密钥生成、分发、销毁应记录日志，销毁时应采用物理粉碎或多次覆写。

8.4.3　安全审计

8.4.3.1　审计范围应覆盖数据访问、设备配置变更、安全事件处置等所有操作。
8.4.3.2　审计日志应至少包含操作人、时间、操作内容、IP 地址、操作终端型号与 MAC 地址、操作结果（成功/失败），日志格式应符合 YD/T 4242 的规定且不可篡改，保存周期不少于 6 个月。
8.4.3.3　应智能化审核审计日志，基于设定审计规则和机器学习模型，自动识别异常行为，重点排查异常操作，如非工作时间修改设备配置、多次失败的登录尝试。
8.4.3.4　发现安全事件时，立即启动应急响应，自动锁定相关操作账号和操作终端，保存日志作为调查依据，并标注危险等级推送告警至运维负责人，负责人应在 24 h 内完成核查，核查结果及处置措施录入审计档案。

9　网络安全管理

9.1　边界防护

9.1.1　收费站机房的生产网络与办公网、第三方接入网络之间应部署应部署符合 GB/T 20281 要求的防火墙或网闸，并配置精细化的访问控制策略。
9.1.2　所有边界防护设备的安全日志应实时、全量接入上级网络安全运营中心，接受统一的安全策略下发与合规性审查。
9.1.3　防火墙应开启状态检测、ACL，不应允许未经授权的 IP 地址访问内网收费服务器。
9.1.4　应定期审查防火墙策略，防火墙访问控制策略应遵循“最小权限”原则，移除过期或冗余规则。
9.1.5　入侵检测应符合包括但不限于以下要求：

——IDS 应实时监测网络异常流量，包括但不限于端口扫描、DDoS 攻击、暴力破解等行为；
——发现安全事件时，告警响应时间应≤5 min，告警信息应同步至运维管理平台并通知安全责任人。

9.2 终端安全

9.2.1 机房内服务器、工作站及运维终端应部署受控的防病毒软件，并每周更新病毒库。
9.2.2 应关闭不必要的端口和服务。
9.2.3 所有终端的安全状态应纳入上级网络安全运营中心的统一资产管理。
9.2.4 运维终端不应接入非授权存储设备；远程运维应通过 VPN 加密通道，并记录所有操作行为。

9.3 接入管控

9.3.1 应启用交换机端口安全策略，对接入设备进行身份验证。
9.3.2 所有网络接入认证日志应同步至上级网络安全运营中心。

9.4 漏洞与补丁管理

9.4.1 应每季度对网络设备、服务器进行至少 1 次全网漏洞扫描，扫描范围应覆盖所有在线资产，发现高危漏洞应经测试验证后及时修补。
9.4.2 漏洞修复过程应形成工单，在运维管理平台中实现从发现、派发、修复到验证的全流程闭环跟踪。
9.4.3 漏洞修复时限应符合以下要求：高危漏洞修复时限≤24 h，中危漏洞修复时限≤72 h，低危漏洞可结合月度维护计划统一处理。
9.4.4 补丁安装前应在测试环境验证，并制定回退方案。
9.4.5 应每年开展 1 次渗透测试，并根据测试结果加固系统。

9.5 网络安全等级保护

9.5.1 收费站收费系统、联网收费系统等核心业务系统的建设应符合 GB/T 25070、GB/T 22239 的规定，其保护等级应不低于等级保护第三级，每年至少开展 1 次等级测评和商用密码应用安全性评估。
9.5.2 等保测评和密评报告、整改记录等文档应统一归档于上级网络安全运营中心的知识库。
9.5.3 应制定网络安全事件应急预案，每年至少开展 1 次应急演练，并根据演练结果修订完善应急预案。应急演练应记录过程，形成演练总结报告。
9.5.4 等级保护对象的定级结果、备案证明、测评报告、整改记录、应急演练记录等文档保存期限不少于 3 年。

9.6 智能化安全要求

9.6.1 收费站机房的防火墙、IDS、终端安全日志等网络安全监测数据应实时、稳定地上传至上级网络安全运营中心。安全告警事件应与运营中心的威胁情报库进行自动比对，并支持一键下发封禁、隔离等应急响应指令。
9.6.2 宜利用运营中心的 AI 分析能力，对本站历史安全数据进行关联分析，主动识别潜在风险并生成优化建议。
9.6.3 宜建立安全响应机制，对常见安全事件实现自动化或半自动化处置，减少人工干预时间。自动化处置操作应记录审计日志，并符合 8.4.3.4 的要求。
9.6.4 应通过安全管理中心对防火墙、入侵检测、终端安全等设备的策略进行集中配置、下发和审计。
9.6.5 应采用自动化工具进行网络资产动态发现与识别，建立资产清单，资产识别准确率不应低于 98%。
9.6.6 宜接入行业或第三方威胁情报，对已知恶意 IP、域名、URL 进行实时比对和阻断。
9.6.7 宜将网络安全告警与智能化巡检系统联动，进行安全事件与设备运行状态（CPU、内存、连接数）的关联分析。

参 考 文 献

[1] GB/T 43208.1—2023 信息技术服务 智能运维 第1部分：通用要求[S].
[2] GB/T 43208.2—2025 信息技术服务 智能运维 第2部分：数据治理[S].
[3] GB/T 44463—2024 互联网数据中心（IDC）总体技术要求[S].
[4] GB/T 51314—2018 数据中心基础设施运行维护标准[S].
[5] GB/T 51409—2020 数据中心综合监控系统工程技术标准[S].
[6] YD/T 4458—2023 数据中心精细化运维技术要求及评估方法[S].
[7] YD/T 4626—2023 数据中心运营管理系统技术要求和智能化分级评估方法[S].
[8] YD/T 6231—2024 数据中心智能化运维综合管控技术要求[S].
[9] YD/T 6515—2025 数据中心基础设施智能化运行管理评估方法[S].
[10] 信息安全等级保护管理办法（公通字〔2007〕43号）
[11] 中华人民共和国保守国家秘密法（中华人民共和国主席令第28号）
[12] 中华人民共和国密码法（中华人民共和国主席令第35号）
[13] 中华人民共和国网络安全法（中华人民共和国主席令第61号）
[14] 中华人民共和国数据安全法（中华人民共和国主席令第84号）
[15] 网络数据安全管理条例（中华人民共和国国务院令第790号）

中华人民共和国团体标准

高速公路收费站机房网络智能化运维管理规范

T/GXAS 1406—2026

广西标准化协会统一印制