

ICS 35.240

CCS L77

# 团体标准

T/JSHLW 003-2026

## 高快速路交通管控智能体系统应用指南

Application guide for agent-based traffic control and management systems on highways and urban expressways

2026-02-25 发布

2026-03-25 实施

江苏省互联网协会 发布

## 目 次

前 言	III
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 缩略语	2
5 总体架构	3
6 功能要求	4
6.1 交通感知功能	4
6.2 数据分析功能	4
6.4 决策处置功能	4
6.5 信息发布功能	5
6.6 系统互联要求	5
6.7 系统管理与运维功能	5
7 性能指标	6
7.1 数据处理性能	6
7.2 控制性能	6
7.3 事件处理性能	6
7.4 系统整体性能	6
8 数据规范	7
8.1 数据分类与格式	7
8.2 数据存储与共享要求	7
9 安全要求	7
9.1 网络安全	7
9.2 数据安全	8
9.3 设备安全	8
9.4 应急安全	9
10 运维管理	9
10.1 日常运维	9
10.2 运维评估与优化	10

## 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》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。

本文件由江苏省互联网协会提出并归口。

本文件起草单位：南京理工大学、江苏省互联网行业联合会、江苏悦达专用车有限公司、中国科学技术大学、华东交通大学、宜春市公路事业发展中心上高分中心、南京凌云科技发展有限公司、江苏省气象信息中心（江苏省气象档案馆）、苏交科集团股份有限公司、江苏智城慧宁交通科技有限公司、南京智慧交通信息股份有限公司。

本文件主要起草人：戚湧、郝冠亚、周竹萍、邵凤明、秦家虎、邓明君、陈思遥、陈璐、黄亮、马麒超、曾招坤、刘剑、高宁波、陈军、杨勇刚、谢文文、张兵、付维明、耿丹、赵小平、姚昌梁、刘金伟、吴晨、张涛。

# 高快速路交通管控智能体系统应用指南

## 1 范围

本文件规定了高速公路及城市快速路交通智能体管控系统（以下简称“管控系统”）的总体架构、功能要求、性能指标、数据规范、安全及运维管理要求等内容。本文件适用于高速公路及城市快速路交通智能体管控系统的规划、设计、建设与运维，也可作为相关技术研发、产品选型的参考依据。

## 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 2894 安全标志及其使用导则

GB/T 28181 安全防范视频监控联网系统信息传输要求

GB/T 33577 智能运输系统 数据字典要求

JT/T 1008 公路网运行监测与服务暂行技术要求

T/ITS 0095 智能交通系统 车路协同 术语

JT/T 606.2 交通信息基础数据元 第 2 部分：公路信息基础数据元

## 3 术语和定义

下列术语和定义适用于本文件。

### 3.1

**高快速路** highways and urban expressways

指高速公路和城市快速路的统称，高速公路是符合国家相关技术标准，专供汽车分向、分车道高速行驶并全部控制出入的公路；城市快速路是城市中有较高车速、为长距离交通服务的重要道路。

### 3.2

**智能体** agent

能够感知环境、进行决策并执行动作的软件或硬件实体，具有自主性、交互性和适应性。

### 3.3

**交通管控智能体系统** intelligent traffic control agent system

融合人工智能、大数据、物联网、车路协同等技术，具备交通状态感知、数据分析研判、信号控制、事件预警与处置、信息发布等功能，能够实现高快速路交通运行智能化管控的综合系统。

### 3.4

### 交通状态感知 traffic state perception

通过各类感知设备采集高快速路交通流参数（流量、速度、密度）、车辆信息（车牌、车型、车辆状态）、道路环境信息（天气、路面状况）等数据的过程。

### 3.5

#### 车路协同 cooperative vehicle-infrastructure system, CVIS

通过先进的无线通信，实现车辆与道路基础设施（如信号灯、摄像头、雷达、边缘计算单元等）之间的实时信息交互与协同感知、协同决策、协同控制，从而提升道路交通安全性、效率和自动化水平的技术体系。

### 3.6

#### 交通事件 traffic incident

影响高快速路正常交通运行的异常情况，包括不限于交通事故、车辆故障、道路施工、交通拥堵、恶劣天气影响、行人或动物闯入、信号灯故障以及大型活动引发的拥堵等。

### 3.7

#### 数据分析研判 data analysis and intelligence assessment

管控系统对采集到的多源感知数据进行清洗、融合、挖掘与分析，形成高质量数据集，运用交通流理论、机器学习等算法，识别交通运行规律、判断交通状态、预测交通流变化趋势及评估交通事件影响范围与程度的过程。

### 3.8

#### 信号控制 traffic signal control

针对高快速路的出入口、互通立交等关键节点，结合交通状态感知数据与数据分析研判结果，通过智能信号控制算法，动态调整信号灯的配时方案，优化交通流分配，减少交通延误，提高节点通行效率的控制方式。

### 3.9

#### 信息发布 information dissemination

管控系统将交通状态信息、交通事件信息、管控措施信息及出行建议等，通过多种渠道向道路使用者、交通管理人员等相关对象实时发布的过程，以引导交通出行，提升出行体验。

## 4 缩略语

下列缩略语适用于本文件。

HTTP/2	车云通信的高效应用层协议（Hypertext Transfer Protocol Version 2）
IDS	入侵检测系统（Intrusion Detection System）
IPS	入侵防御系统（Intrusion Prevention System）
JSON	对象表示法（一种数据交换格式）（JavaScript Object Notation）
LSTM	长短期记忆网络（Long Short-Term Memory）
MAC	为网络接口分配的唯一地址编码（Medium Access Control）
MQTT	轻量级、低功耗、低带宽的即时通信协议（Message Queuing Telemetry Transport）

TCP	传输控制协议 (Transmission Control Protocol)
UDP	用户数据报协议 (User Datagram Protocol)
URLLC	超可靠低时延通信 (Ultra-Reliable Low-Latency Communication)
VIN	车辆识别代号 (Vehicle Identification Number)
VLAN	虚拟局域网 (Virtual Local Area Network)
XML	可扩展标记语言 (Extensible Markup Language)

## 5 总体架构

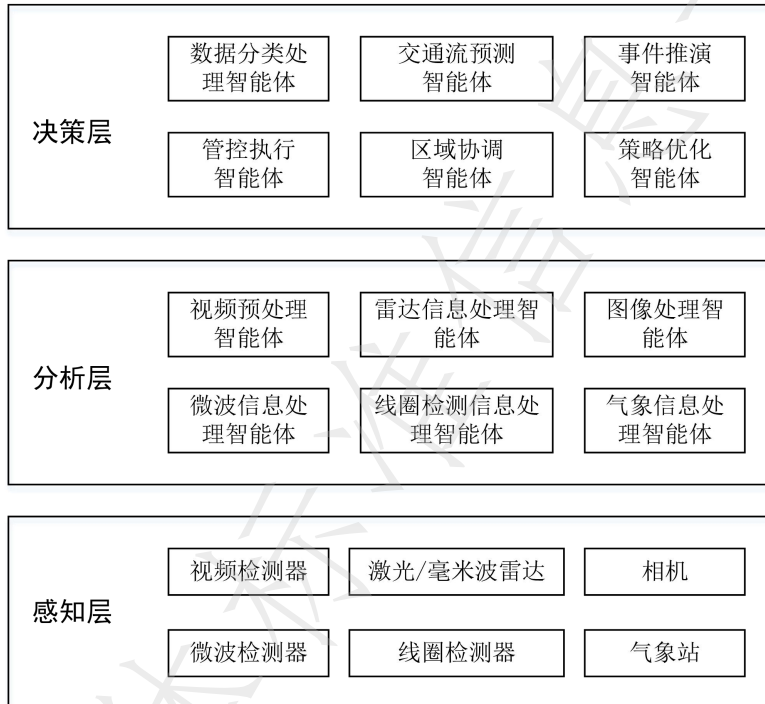


图 1 系统架构图

如图 1 所示，高快速路交通智能体管控系统采用“感知层 - 分析层 - 决策层”三层架构，各层级协同工作，实现数据的高效流转、处理与应用，具体如下：

**感知层：**作为系统与物理世界交互的“接口”，能够控制各类感知设备，包括：视频检测器、微波检测器、线圈检测器、雷达、气象站、车牌识别相机等，负责采集交通流、车辆、环境等数据。

**分析层：**功能模块可部署于边缘计算设备或云平台端，具备承担数据预处理、实时计算功能，对前端感知设备采集的数据进行实时清洗、过滤与融合。边缘端设备的使用能够快速处理本地数据、及时执行相应运算，降低上传云端数据量，提高系统实时性。

**决策层：**作为系统的“大脑中枢”，主要负责海量数据的存储、集中管理、深度分析与全局决策。部署大数据存储与管理平台、人工智能分析引擎、交通决策支持系统等核心组件，可通过管理不同的智能体设备实现交通流管控、全局交通优化方案制定、系统运维管理及与其他跨部门平台的数据交互与共享。

## 6 功能要求

### 6.1 交通感知功能

**多源数据采集：**应支持通过视频检测器、微波检测器、线圈检测器、激光雷达等多种感知设备，采集交通流参数（流量、速度、密度、车头时距）、车辆信息（车牌、车型、颜色、VIN、行驶轨迹、是否超载超限）、道路环境信息（天气类型、降雨量、能见度、路面温度、路面湿度、是否有积雪/结冰/积水）等数据；采集频率应可配置。

**数据质量控制：**应具备数据清洗、异常值剔除与数据补全功能。可通过算法识别并过滤感知设备故障、恶劣天气干扰等导致的异常数据；对于缺失的数据，采用插值法、机器学习预测等方式进行补全，确保感知数据的准确性与完整性，交通流参数数据准确率不低于 90%、正常光照条件下车牌识别准确率不低于 95%。

### 6.2 数据分析功能

**多源数据接入：**需同时支持 MQTT、HTTP/2、TCP/UDP 等协议；同时支持多终端数据接入，满足 URLLC 要求。

**清洗与标准化：**识别并处理脏数据，将来自不同厂商、不同协议的数据转化为系统内部统一的标准化格式；应具备异常值、缺失值的处理能力。

**关联与融合：**需具有对同一个目标的多个传感器观测值进行数据融合的能力；具备提取不同数据的特征（包括图像特征、点云特征、信号特征）进行联合分析的能力。

### 6.4 决策处置功能

**事件自动检测：**基于视频分析、雷达探测、车辆轨迹异常识别等技术，实现交通事件的自动检测。可检测的事件类型包括交通事故、车辆故障、道路施工、交通拥堵、路面障碍物等，白天正常天气条件下检测准确率应不低于 90%、夜间或恶劣天气条件下不低于 80%，检测延迟不超过 10 秒。

**交通状态评估：**基于感知数据，运用交通流理论与机器学习算法，应能实时评估高快速路各路段的交通状态，划分畅通（车速 $\geq$ 设计时速 80%）、基本畅通（车速为设计时速 60%-80%）、轻度拥堵（车速为设计时速 40%-60%）、中度拥堵（车速为设计时速 20%-40%）、严重拥堵（车速小于设计时速 20%）五个等级，并以可视化方式展示。

**事件影响分析：**当发生交通事件时，系统应具备快速评估事件对交通流的影响范围、影响程度及预计恢复时间，并能够模拟不同处置方案下的交通流恢复过程。

**分级预警：**根据事件的严重程度，将事件划分为一般预警（轻微车辆故障、短时间拥堵）、较重预警（一般交通事故、较长时间拥堵）、严重预警（重大交通事故、危险品泄漏、大范围拥堵）三个等级。不同等级的预警采用不同的通知方式，通知对象包括交通巡逻人员、养护人员、指挥中心调度员等相关责任人。

**处置流程指引与跟踪：**针对不同类型与等级的事件，系统内置标准化的处置流程指引，

为处置人员提供操作指导；同时，实时跟踪事件处置进度，记录处置时间节点，并可生成处置报告，便于后续复盘与优化。

**动态配时优化：**针对高快速路出入口等节点的信号灯，系统应支持基于实时交通流数据与预测结果的动态配时。可根据不同方向的车流需求，自动调整信号灯的绿灯时长、红灯时长与黄灯时长，减少车辆排队长度与等待时间；在交通高峰期与平峰期，分别采用不同的配时策略，实现通行效率最大化。

**协调控制：**对于相邻的多个信号灯节点，需支持协调控制功能。可通过优化各节点信号灯的相位差，减少车辆在节点间的停车次数，提升整体路段的通行效率；协调控制范围可根据实际交通需求灵活调整。

**手动干预与预案控制：**需支持交通管理人员通过控制台进行手动干预，临时调整信号灯配时方案；系统可内置多种预设预案，在特定场景下应能快速启用，提高应急响应速度。

## 6.5 信息发布功能

**多渠道发布：**应支持通过多种渠道向道路使用者与相关人员发布信息，主要包括：户外显示设备、移动终端、交通广播、短信平台、官方网站等，发布全局交通信息与重要预警通知，覆盖更广泛的受众。

**信息更新与准确性：**信息发布需保证实时性与准确性，当交通状态或事件情况发生变化时，需在 30 秒内更新相关信息，避免误导道路使用者；发布的信息应语言简洁、表述准确，避免模糊不清或错误内容。

## 6.6 系统互联要求

**内部互联：**感知层、预测层、决策层之间通过有线或无线网络实现互联互通，确保数据传输的实时性、可靠性与安全性。采用标准化的通信协议，保障各层级设备与平台之间的兼容与协同。

**外部接口：**系统需预留标准化接口，支持与外部系统的数据交互与业务协同。接口需符合 GB/T 28181、JT/T 1008 相关标准，确保数据格式统一、交互安全合规。

## 6.7 系统管理与运维功能

**设备管理：**支持对系统内所有感知设备、执行设备、边缘计算节点、服务器等硬件设备的统一管理。可实时监测设备的运行状态，当设备出现故障时，自动发出故障告警；系统应支持设备信息的录入、修改、删除与查询，建立完整的设备档案。

**用户管理：**支持分级用户管理，根据用户角色分配不同的操作权限，确保系统操作的安全性与规范性。可实现用户账号的创建、注销、密码重置、权限修改等功能，并记录用户的操作日志，便于审计与追溯。

**日志管理：**系统应能自动记录各类操作日志，日志内容包括时间、设备号、操作人、操作内容、结果状态等信息。日志存储时间不低于 1 年，支持按时间范围、操作类型、关键字

等条件进行查询、导出与统计分析，为系统故障排查、责任追溯与优化提供依据。

**系统性能监测与优化：**实时监测系统的运行性能，包括：数据处理速度、响应时间、网络带宽占用率、服务器资源利用率等，当性能指标超出预设阈值时，发出性能告警；同时，支持对系统性能进行定期分析，识别性能瓶颈，并提供优化建议，确保系统长期稳定运行。

## 7 性能指标

### 7.1 数据处理性能

**数据采集速率：**系统每秒可处理的感知数据量不低于 100MB，支持同时接入不少于 100 路视频监控设备及其他类型的感知设备。

**数据处理延迟：**边缘层对实时感知数据的预处理（清洗、融合）延迟不超过 1 秒；云端层对数据的深度分析延迟不超过 5 秒；数据查询响应时间不超过 3 秒（单条查询）、不超过 10 秒（批量查询，数据量≤10 万条）。

**数据存储容量与可靠性：**云端存储系统的总容量不低于 300TB 并支持扩展；采用冗余存储技术，数据存储可靠性不低于 99.99%，确保数据不丢失；历史数据的保存期限可配置，交通流数据保存不低于 6 个月，事件数据、操作日志保存不低于 1 年。

### 7.2 控制性能

**信号控制响应时间：**从系统接收到交通流数据变化到信号灯配时方案调整完成的总响应时间不超过 10 秒；手动干预信号灯配时的响应时间不超过 5 秒。

**控制精度：**动态配时优化后，节点的车辆平均等待时间较固定配时方案减少不低于 20%；高峰通过率不低于 50%。

**稳定性：**信号控制系统连续无故障运行时间不低于 1,000 小时。

### 7.3 事件处理性能

**事件检测准确率与延迟：**在白天正常天气条件下，交通事故、车辆故障等主要事件的检测准确率不低于 90%，路面障碍物、小型施工的检测准确率不低于 85%；夜间或恶劣天气条件下，主要事件的检测准确率不低于 80%。事件检测延迟（从事件发生到系统发出预警）不超过 30 秒，重大事件的检测延迟不超过 20 秒。

**事件处置响应时间：**系统发出事件预警后，相关责任人接收通知的时间不超过 1 分钟。

### 7.4 系统整体性能

**并发访问能力：**支持不少于 50 个用户同时登录系统进行操作，且系统响应时间不超过 3 秒；支持不少于 1000 个移动终端同时接收信息推送，信息推送成功率不低于 98%。

**可用性：**云端平台可用性不低于 99.95%，边缘层设备可用性不低于 99.9%，终端感知设备可用性不低于 99%。

**扩展性：**系统支持硬件设备的灵活扩展，新增设备接入时无需对现有系统架构进行大规模改造；支持功能模块的扩展，可通过插件化方式集成。

## 8 数据规范

### 8.1 数据分类与格式

根据数据来源与用途，将管控系统的数据分为以下几类，并明确各类数据的格式要求：

**交通流数据：**包括流量、速度、密度、车头时距等参数。数据格式宜采用 JSON 或 XML，每条数据需包含采集时间（格式：YYYY-MM-DD HH:MM:SS）、采集设备 ID、路段编号、车道号、流量（单位：辆/分钟）、速度（单位：km/h，保留 1 位小数）、密度（单位：辆/km）、车头时距（单位：秒，保留 1 位小数）等字段。

**车辆数据：**包括车牌、车型、颜色、VIN 码、行驶轨迹、超载超限信息等。数据格式采用 JSON，每条数据需包含采集时间、采集设备 ID、车牌号码、车牌颜色、车型、VIN 码、行驶轨迹、是否超载超限等字段。

**事件数据：**包括事件类型、发生时间、发生位置、严重程度、处置进度等。数据格式采用 JSON，每条数据需包含事件 ID、事件类型（交通事故、车辆故障、道路施工）、发生时间、发生位置（经纬度坐标 + 路段名称 + 车道号）、严重程度（一般/较重/严重）、事件描述、处置状态（未处置/处置中/已完成）、处置责任人、处置时间节点等字段。

**控制指令数据：**包括信号灯配时指令、信息发布指令、车道控制指令等。数据格式采用 JSON，每条指令需包含指令 ID、指令类型、接收设备 ID、指令内容、指令下发时间、指令执行状态（未执行/执行中/已执行）、执行结果反馈等字段。

### 8.2 数据存储与共享要求

**数据存储要求：**数据存储需采用分布式存储架构，支持容量扩展与负载均衡；存储系统需具备数据备份功能，定期进行全量备份，每周进行 1 次增量备份，备份数据需异地存储，保存期限不低于 1 年；对于敏感数据，需采用加密存储，并严格控制访问权限，防止数据泄露。

**数据共享要求：**数据共享需遵循“合法、合规、安全、可控”的原则，共享范围与权限需根据数据敏感程度与合作需求明确界定；共享数据需符合 GB/T 33577、JT/T 606.2 的要求，确保接收方能够正常解析与使用；数据共享过程中需签订数据共享协议，明确双方的权利与义务，包括数据用途、使用期限、保密责任、违约责任等；同时，需对数据共享过程进行日志记录，便于追溯与审计。

## 9 安全要求

### 9.1 网络安全

**网络隔离与访问控制：**采用防火墙、网闸等设备，实现管控系统与外部网络、内部不同层级网络之间的隔离，防止未经授权访问；在网络边界部署 IDS 与 IPS，实时监测与拦截网络攻击；采用 VLAN 技术，对不同功能区域的网络进行划分，限制不同区域之间的非法数据访问。

**身份认证与权限管理：**所有接入系统的设备与用户均需进行身份认证。设备采用数字证书认证或 MAC 地址绑定方式，用户采用“用户名 + 密码 + 动态验证码”的多因素认证方式，认证失败次数超过 5 次时，账号/设备需被临时锁定（锁定时间不低于 30 分钟）；基于最小权限原则，为不同角色的用户与设备分配相应的操作权限，禁止超权限操作，权限变更需经过审批流程，并记录变更日志。

**数据传输安全：**数据在网络传输过程中，需采用加密技术，确保数据的机密性与完整性；采用数字签名技术，对重要数据进行签名，接收方需验证签名有效性，防止数据被篡改或伪造；定期对网络传输链路进行安全检测，及时发现并修复漏洞。

## 9.2 数据安全

**数据分类分级保护：**根据数据的敏感程度（公开数据、内部数据、敏感数据、核心数据），对系统数据进行分类分级，并采取相应的保护措施。公开数据可自由发布；内部数据仅对内部授权人员开放；敏感数据需采用加密存储与访问控制；核心数据需采用多重加密与备份，防止丢失或泄露。

**数据脱敏与匿名化：**对于涉及个人隐私或商业秘密的数据，在数据共享或对外发布前，需进行脱敏或匿名化处理。常用的处理方式包括数据替换、数据屏蔽、数据删除，确保处理后的数据无法关联到具体个人或企业，同时不影响数据的统计与分析用途。

**数据备份与恢复：**按照本文件 8.3 节的要求，定期进行数据备份，并对备份数据的有效性进行验证；制定数据恢复预案，明确数据丢失或损坏后的恢复流程、责任人员与时间要求。对于重要数据，需确保在 1 小时内完成恢复，恢复数据的完整性不低于 99.9%；同时，定期开展数据恢复演练，提升应急处置能力。

## 9.3 设备安全

**设备接入安全：**所有接入管控系统的感知设备、执行设备、边缘计算节点等硬件设备，经过严格的安全检测，符合相关安全标准后方可接入；设备接入时需进行身份认证，禁止未经授权设备接入系统；定期对设备固件进行更新，修复已知漏洞，更新过程需采用加密传输与签名验证，防止固件被篡改。

**设备物理安全：**设备的安装位置需选择安全、稳定的环境，避免受到自然灾害、人为破坏的影响；对于户外安装的设备，需具备防水、防尘、防雷、防腐蚀、抗电磁干扰的能力，户外设备防护等级不低于 IP65、室内设备防护等级不低于 IP30；设备机箱需加装防盗锁，重要设备需安装在带门禁的机房或机柜内，机房需配备监控摄像头与入侵报警装置。

**设备运行安全：**实时监测设备的运行状态，包括硬件状态与软件状态，当设备出现异常时，及时发出告警并通知运维人员；定期对设备进行巡检与维护，清洁设备、检查线路连接、测试设备功能，确保设备长期稳定运行；对于故障设备，需及时进行维修或更换，减少设备停运时间。

#### 9.4 应急安全

**应急预案制定：**制定完善的应急安全预案，涵盖网络攻击、数据泄露、设备大规模故障、自然灾害等各类突发事件场景。预案内容包括应急组织机构与职责、应急响应流程、应急资源配置、应急处置措施、后期评估与改进机制等。

**应急演练与培训：**定期组织应急安全演练（每半年至少 1 次），模拟不同类型的突发事件，检验应急预案的可行性与有效性，提升应急团队的协同处置能力；加强对系统管理人员、运维人员、使用人员的安全培训（每季度至少 1 次），培训内容包括安全意识、安全操作规范、应急处置流程、安全技术知识等，确保相关人员具备应对突发事件的能力。

**应急响应与恢复：**当发生突发事件时，按照应急预案启动相应级别的应急响应，迅速组织人员开展处置工作。

### 10 运维管理

#### 10.1 日常运维

- a) **巡检制度：**建立完善的日常巡检制度，明确巡检频率、巡检内容、巡检人员与巡检记录要求。
- b) **巡检频率：**每日进行 1 次日常巡检（远程监测为主），每周进行 1 次现场巡检，每月进行 1 次全面巡检；在恶劣天气、交通高峰期、重大活动期间，增加巡检频率。
- c) **巡检内容：**
  - 1) **远程监测：**通过系统管理平台，监测设备运行状态、数据采集与传输情况（、系统功能运行情况、安全状态；查看系统日志，分析是否存在异常记录。
  - 2) **现场巡检：**检查户外设备的外观是否完好，有无损坏、倾斜、遮挡；检查设备固定是否牢固，线缆连接是否松动、破损，防水处理是否完好；检查机房/控制柜的环境，查看消防设备、门禁系统、监控设备是否正常；测试设备功能，确保设备工作正常。
  - 3) **巡检记录：**巡检人员需填写《日常巡检记录表》，详细记录巡检时间、巡检内容、发现的问题、处理情况记录、巡检人员签字；《日常巡检记录表》需每日归档，每周汇总，每月进行分析，为后续运维工作提供依据。
- d) **定期维护：**
  - 1) **设备清洁：**每月对户外设备进行清洁，去除灰尘、污渍，确保设备正常工作；每季度对机房/控制柜进行清洁，清理灰尘、杂物，检查通风散热设备。

- 2) **设备校准**: 每 3 个月对感知设备进行校准, 使用标准设备进行对比测试, 调整设备参数, 确保采集数据的准确性; 每 6 个月对信号灯的亮度、色度进行校准, 确保符合 GB 2894 的要求。
- 3) **软件维护**: 每月对系统软件进行漏洞扫描与更新, 安装最新的安全补丁, 关闭不必要的服务与端口; 每季度对数据库进行优化, 提升数据查询与处理效率; 定期备份系统配置参数与重要数据, 确保数据安全。
- 4) **故障维护**: 当设备或系统出现故障时, 运维人员需及时响应, 按照“故障定位 - 故障排除 - 恢复运行 - 原因分析”的流程进行处理。
- 5) **故障定位**: 通过远程监测日志、现场检查设备状态、使用测试工具等方式, 快速定位故障原因。
- 6) **故障排除**: 根据故障原因, 采取相应的排除措施。
- 7) **恢复运行**: 故障排除后, 测试设备或系统功能, 确保恢复正常运行; 对于信号控制、信息发布等关键功能, 需进行全面测试, 避免影响交通运行。
- 8) **原因分析**: 故障处理完成后, 分析故障产生的根本原因, 记录在《故障处理记录表》中, 并采取预防措施, 避免同类故障再次发生。

## 10.2 运维评估与优化

- a) **运维评估**: 定期对运维工作进行评估, 分析运维效果与存在的问题, 为运维优化提供依据。
  - 1) **评估频率**: 每季度进行 1 次月度运维评估, 每年进行 1 次年度运维评估。
  - 2) **评估内容**: 包括运维工作完成情况、系统运行状态、运维成本、用户满意度。
  - 3) **评估方法**: 采用数据统计分析、现场检查、问卷调查、专家评审等多种方法进行评估。
- b) **运维优化**: 根据运维评估结果, 结合交通需求变化与技术发展, 对运维工作进行持续优化。
  - 1) **优化内容**: 包括运维流程优化、运维资源配置优化、技术优化、应急预案优化。
  - 2) **优化实施**: 制定运维优化方案, 明确优化目标、优化措施、责任人员与实施时间; 在优化方案实施过程中, 加强监测与评估, 及时调整优化措施; 优化完成后, 总结优化效果, 将有效的优化措施纳入日常运维制度, 实现运维工作的持续改进。