ICS 35.020
CCS L 77

T/CS

团 体 标 准

T/CS 226—2025

城市隧道智慧运维综合管控平台技术规范

Technical specifications for the integrated control platform for smart operation and maintenance of urban tunnels

2025-12-19 发布 2025-12-19 实施

中国商品学会 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　总体要求 1
5　架构 1
6　功能 2
7　性能 3
8　接口 4
9　调试和评估验收 4
10　安全管理 4
11　运维 5
参考文献 7

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。

本文件由苏州申亿通智慧运营管理有限公司提出。

本文件由中国商品学会归口。

本文件起草单位：苏州申亿通智慧运营管理有限公司、苏州通标城市建设运营有限公司、中亿丰路桥建设有限公司、苏州高新城市运营管理有限公司、苏州工业园区市政服务集团有限公司、江苏东吴路桥建设集团有限公司。

本文件主要起草人：祁伟林、陈伟、刘刚、袁媛、龚彬、徐杲再、赵凯岩、高平、王圣康、朱宏亮、曲林、程传金、潘忠良、陈博、李俊剑、严振瑞、陆明哲、张辉、范超军。

城市隧道智慧运维综合管控平台技术规范

1 范围

本文件规定了城市隧道智慧运维综合管控平台的总体要求、架构、功能、性能、接口、调试和评估验收、安全管理和运维。

本文件适用于城市隧道智慧运维综合管控平台的建设和管理。

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 20272 信息安全技术 操作系统安全技术要求

GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求

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 32905 信息安全技术 SM3密码杂凑算法

GB/T 32907 信息安全技术 SM4分组密码算法

GB/T 35276 信息安全技术 SM2密码算法使用规范

GB/T 41479 信息安全技术 网络数据处理安全要求

3 术语和定义

本文件没有需要界定的术语和定义。

4 总体要求

4.1 平台应提供清晰、简洁的人机交互界面，各个模块的界面风格和操作习惯应一致，操作应易学易用，应能使平台用户快速找到所需功能和信息。

4.2 平台应能适应不同终端设备，在不同分辨率和屏幕尺寸下应能呈现良好显示效果。

5 架构

平台由业务应用层、基础支撑层、数据层组成：

a) 业务应用层：包括多项目系统、单项目系统；

b) 基础支撑层：包括地理信息系统（GIS）引擎、存储过程、数据缓存、读写数据库等；

c) 数据层：包括基础数据、图集数据、监测数据、安全资料数据、业务数据等；

d) 感知层：包括传感器、数据采集设备等。

6 功能

6.1 多项目系统功能

6.1.1 项目管理

应支持对多个单隧道项目进行组合划分，实现区域性养护项目的统一管理。

6.1.2 系统管理

系统管理包括组织管理、角色管理、用户管理、岗位管理、字典管理、系统日志功能，提供养护相关方的组织结构信息，为不同的角色、用户和岗位设置相应的权限。

6.1.3 标准管理

标准管理包括管理单元、设施分类、设备分类、监测类型、缺陷类型、巡检配置、班组管理、物资分类、物资管理、车辆管理等功能，提供各管理单元基础信息及附件信息，设置各类字典项与巡检条目，建立班组、物资、车辆等台账，实现信息的统一化管控。

6.2 单项目系统功能

6.2.1 基础数据管理

应根据需求进行配置，包含管理单元、管理编码、设备管理、设施管理、班组管理、文档管理、排班管理、车辆管理、物资管理、测点组管理、测点管理、测点数据、预设结构图等功能模块，对隧道、人员、物资等信息进行全面管理。

6.2.2 安全管理

应集中上传应急排班、安全检查、应急资料及安全会议等各类资料，实现信息电子化归档。

6.2.3 计划管理

应预设标准化业务流程，制定业务计划，实现年计划、月计划、周计划的计划编排管理。

6.2.4 运营管理

应提供事件管理、事件统计、交通流量、投诉管理等功能模块，实现运营数据的分析、查询和展示：

a) 事件管理：实时上报记录突发事件，包括牵引、封道及路损等信息；
b) 事件统计：对事件进行列表统计，呈现运营事件；
c) 交通流量：对交通流量数据进行管理和分析展示，为交通流量变化和高峰期隧道运维提供指导；
d) 投诉管理：提供各类投诉的查看、回复、审核、整改并生成作业单。

6.2.5 养护管理

应提供维养管理、缺陷管理、缺陷统计、封道管理等功能模块，实现缺陷及养护作业单全过程跟踪管理：

a) 维养管理：提供养护或维修作业单的线上流程操作，包括分配、确认、安全交底、执行、验收，实现维养作业单的标准化管理；

b) 缺陷管理：对日常巡检、专项检查、监测预警、投诉等方式发现的缺陷进行上报，并根据缺陷生成维修作业单；
c) 缺陷统计：对养护管理中的缺陷进行统计；
d) 封道管理：提供围封或解封作业单的线上流程操作，包括分配、确认、安全交底、执行、验收，实现封道作业的标准化管理。

6.2.6 巡检管理

6.2.6.1 应提供巡检作业、巡检记录、巡检配置、巡检路线等功能，实现巡检作业的任务分配、处置及再分配，并支持按不同维度查询巡检记录。
6.2.6.2 应能对规定巡检设备的巡检项内容进行配置，完成巡检计划路线组及路线类型的设置。

6.2.7 结构监测

应能通过接入健康监测设备数据，对设施结构状态实时展示，对监测数据超出阈值的情况进行预警，实时掌握设施结构健康状态。

6.2.8 机电监测

应接入中控操作平台监控系统、通讯系统、消防系统、通风系统、排水系统、供配电系统、照明系统、环境监控等各大机电系统数据，进行可视化展示，当设备出现故障报警、消防报警、泵房液位超限报警、失电报警等各类突发异常事件时及时弹框显示事故位置、类型等信息。

6.2.9 环境监测

应支持路面温湿度变化的可视化、信息化监控和管理，对监测数据超出阈值的情况进行预警，实现对道路通行状况的精准感知。

6.2.10 积水监测

应在隧道最深处设置液位监测设备、入口处安装液位显示屏，并将数据同步传输至管控平台，实时监测预警积水水位高低。

6.2.11 车流监测

应通过感应线圈、微波雷达、视频分析、激光雷达等方式对隧道车流量和车速进行监测并集成展示。

6.2.12 预警信息

应统计结构、机电、环境、积水等监测预警信息，实现对各类监测预警信息的统一管理。

6.2.13 全寿命评价

应从土建结构、机电系统、附属设施、运维服务等多维度，对隧道进行综合评价。

7 性能

7.1 感知层传感器和数据采集设备应能按设定的频率（最长不超过 5 min）实时采集隧道数据，对于关键部位和重要参数，数据应实时采集。

7.2 数据从感知层传输到数据层的延迟应不超过 1 s，在网络信号较弱或数据传输量达到 5G 的情况下，数据传输延迟应不超过 3 s。
7.3 数据传输过程中应确保数据的完整性和准确性。对于因网络故障或其他原因导致的数据传输失败，系统应支持自动重传，确保数据不丢失。
7.4 数据层应为每台视频监控设备配备不少于 1 T 的数据储存容量，能够满足城市隧道全寿命周期数据的长期存储需求。根据城市隧道规模和数据增长趋势，合理规划数据存储容量，确保数据存储的扩展性和可持续性。
7.5 平台应具备高效的数据处理能力，能实时对至少 1 500 条隧道数据进行分析和处理。
7.6 平台应具备高可用性，通过采用冗余设计、负载均衡、故障自动切换等技术手段，确保系统在出现硬件故障、软件错误或网络中断等情况下能够快速恢复正常运行，保障隧道养护工作的连续性。
7.7 平台应建立完善的数据备份与恢复机制，定期对平台数据进行全量备份和增量备份。当系统出现数据丢失或损坏时，能够在 1 h 内完成数据恢复，确保数据的安全性和完整性。

8 接口

8.1 应具备与第三方平台数据交互的数据接口。
8.2 应预留第三方平台（软件）提供二次开发所需的接口服务。
8.3 可使用超文本传输协议（HTTP）、超文本传输安全协议（HTTPS）等传输协议，可参照 GB/T 38154 相关要求并结合实际情况，制定数据接口规范。

9 调试和评估验收

9.1.1 应在平台安装完成后进行调试。
9.1.2 调试前应具备下列条件：
a) 平台软件已按设计要求安装完毕；
b) 已制定调试和试运行方案；
c) 根据使用说明书校验功能正常。
9.1.3 平台建成后应在第三方功能、性能、安全测试和网络安全等级保护测评后，进行初步验收，初步验收通过之后，转入试运行。
9.1.4 平台连续、安全、稳定试运行 1 个月后，组织竣工验收。验收不合格的应限期整改，整改完毕后进行试运行、复验；复验不合格，应再次整改并试运行、复验，直至验收合格。

10 安全管理

10.1 数据安全

10.1.1 平台中的敏感数据在传输和存储过程中应进行加密处理，按 GB/T 35276、GB/T 32905、GB/T 32907 的要求采用 SM2、SM3、SM4 国密算法加密，确保加密的安全性和可靠性，防止数据被窃取和篡改。
10.1.2 数据备份和恢复过程应采取安全防护措施，防止备份数据被非法获取和篡改。备份数据应存储在安全可靠的存储介质中，并定期进行恢复测试，确保数据备份和恢复的有效性和安全性。
10.1.3 应由授权主体建立数据访问控制机制，根据用户的角色和权限，对数据进行分级管理和授权访

问。只有经过授权的用户才能访问相应的数据，确保数据的保密性和安全性。同时，系统应具备操作日志记录功能，对用户的数据访问操作进行详细记录，以便进行审计和追溯。

10.1.4 应具备自动对任务处理中产生的详细操作和数据进行生成日志的能力。

10.1.5 数据处理应符合 GB/T 41479 的要求。

10.2 网络安全

10.2.1 平台网络安全等级保护应至少符合 GB/T 22239—2019 规定的第三级安全要求。

10.2.2 在平台的网络边界处，应部署防火墙、入侵检测系统（IDS）、入侵防御系统（IPS）等网络安全设备，对网络流量进行实时监测和过滤，防止外部非法网络访问和攻击。应定期对网络安全设备进行升级和维护，确保其防护能力的有效性。

10.2.3 应对平台内部不同区域的网络进行划分和隔离，根据业务需求和安全级别，设置不同的访问权限，防止网络安全事件的扩散和蔓延。

10.2.4 应建立网络安全审计系统，对平台网络中的所有操作进行实时审计和记录，包括网络访问、数据传输、用户登录等操作。通过对审计数据的分析，及时发现网络安全隐患和异常行为，采取相应的措施进行处理，保障网络安全。

10.3 系统安全

10.3.1 应选用符合 GB/T 20272 要求的操作系统。操作系统应及时安装安全补丁，定期进行系统漏洞扫描和修复，确保操作系统的安全性。

10.3.2 应关闭不必要的系统服务和端口，限制系统用户的权限，防止操作系统被攻击和入侵。

10.3.3 对平台的应用程序应进行安全测试和漏洞扫描，包括代码审查、安全漏洞检测、渗透测试等，及时发现和修复应用程序中的安全漏洞。

11 运维

11.1 运维人员

11.1.1 平台应安排专人进行管理，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。

11.1.2 平台应具备用户分层分类功能，满足不同用户不同权限的需求。

11.1.3 技术运维人员应有从事平台运维的能力。

11.1.4 平台运维人员应遵从安全管理规定，定期进行安全意识教育和培训。

11.2 运维安全

11.2.1 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。

11.2.2 应建立完善的运维保障机制，配备专门的运维人员。

11.2.3 应建立系统安全管理制度，对系统安全策略、安全配置、日志管理等方面做出具体规定。

11.2.4 应依据操作手册对系统进行维护，详细记录操作日志，不允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。

11.2.5 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。

11.2.6 运维人员账号应实行权限管理，定期修改账号密码。

11.3 运维制度

11.3.1 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。

11.3.2 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。

11.4 软件和数据维护

11.4.1 应对应用系统与数据资源进行管理和维护，根据设施、设备、物资、车辆等管理内容变化情况，及时进行相应的更新，保证系统正常运行。

11.4.2 应建立数据维护和更新机制，保证设施、设备、物资、车辆等信息数据的安全性、完整性。

11.5 应急处置

11.5.1 应制定平台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，确保平台安全高效运行。

11.5.2 聘请专业人员定期对平台进行巡检，发现问题应及时处理。

参 考 文 献

[1] GB/T 38154 重要产品追溯 核心元数据