

团 体 标 准

T/QGCML XXXX—2025

景区综合管理监测预警系统技术要求

Technical Requirements for Integrated Management Monitoring and Early Warning
System in Tourist Scenic Areas

（征求意见稿）

2025 - 05 - 10 发布

2025 - 05 - 25 实施

全国城市工业品贸易中心联合会 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 总体要求 1

5 系统架构要求 2

6 功能要求 2

7 安全要求 3

8 运维管理 3

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。

本文件由全国城市工业品贸易中心联合会提出并归口。

本文件起草单位：

本文件主要起草人：

景区综合管理监测预警系统技术要求

1 范围

本文件规定了景区综合管理监测预警系统技术要求的术语和定义、总体要求、系统架构要求、功能要求、安全要求、运维管理。

本文件适用于景区综合管理监测预警系统的设计、运行和维护。

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 信息安全技术 网络安全等级保护基本要求
GB/T 35678 公共安全 人脸识别应用 图像技术要求
DZ/T 0439 地质灾害监测预警设备检测技术要求
DZ/T 0460 地质灾害自动化仪器监测预警规范

3 术语和定义

GB/T 35678 界定的以及下列术语和定义适用于本文件。

3.1

景区综合管理监测预警系统 scenic area integrated management monitoring and early warning system

利用物联网、大数据、人工智能、地理信息系统等技术，对景区内的人员、设施、环境、资源等进行全面监测、分析和管理，实现风险预警、应急指挥、决策支持等功能的信息系统。

3.2

数据采集 data collection

通过传感器、摄像头、数据接口等设备和手段，获取景区内各类数据的过程。

4 总体要求

4.1 先进性

系统应采用先进的技术架构和设备，运用成熟的物联网、大数据、人工智能、地理信息系统等技术，确保系统在功能、性能和可靠性等方面具有领先水平，能够适应景区未来发展的需求。

4.2 实用性

系统应紧密围绕景区的实际管理需求进行设计和开发，功能应实用、便捷，操作应简单易懂，能够有效解决景区在人员管理、设施维护、环境监测、资源保护等方面的问题，提高景区的管理效率和服务质量。

4.3 可靠性

系统应具备高可靠性，采用冗余设计、备份机制等技术手段，确保系统在硬件故障、网络中断、软件异常等情况下能够持续稳定运行，数据不丢失、不损坏，保障景区的正常运营。

4.4 安全性

系统应高度重视信息安全，采取完善的安全防护措施，包括网络安全、数据安全、用户认证授权等，防止数据泄露、篡改和非法访问，确保景区和游客的信息安全。

4.5 可扩展性

系统应具有良好的可扩展性，采用模块化设计，能够方便地增加新的功能模块和设备，适应景区规模扩大、业务拓展和技术升级的需求，同时能够与其他相关系统进行无缝对接和数据共享。

4.6 兼容性

系统应具备广泛的兼容性，能够支持不同厂家、不同类型的硬件设备和软件系统，包括传感器、摄像头、服务器、数据库等，确保系统的集成和部署能够顺利进行。

5 系统架构要求

5.1 总体架构

系统总体架构应采用分层设计，包括数据采集层、数据传输层、数据处理层、应用层和用户层，各层之间应相互独立、协同工作，实现数据的采集、传输、处理、存储和应用。

5.2 数据采集层

数据采集层负责采集景区内各类数据，包括但不限于以下内容：

- a) 人员数据：通过门禁系统、票务系统、视频监控等设备采集游客和工作人员的数量、位置、行为等数据。
- b) 设施数据：通过传感器、智能电表、智能水表等设备采集景区内各类设施（如游乐设施、照明设施、给排水设施等）的运行状态、能耗等数据。
- c) 环境数据：通过气象站、空气质量监测站、水质监测站等设备采集景区内的气象、空气质量、水质等环境数据。
- d) 资源数据：通过卫星遥感、无人机航拍、地面监测等手段采集景区内的自然资源（如森林、植被、地质等）和文化资源（如文物古迹、历史建筑等）的相关数据。

5.3 数据传输层

数据传输层负责将数据采集层采集到的数据传输到数据处理层，应采用可靠的传输协议和网络技术，确保数据传输的实时性、准确性和完整性。

5.4 数据处理层

数据处理层负责对传输过来的数据进行清洗、存储、分析和挖掘，为应用层提供数据支持。

5.5 应用层

应用层应提供丰富的业务应用功能，包括但不限于以下内容：

- a) 综合监测：对景区内的人员、设施、环境、资源等进行实时监测，以图表、地图等形式直观展示监测数据和状态，提供异常情况的实时报警功能；
- b) 预警管理：基于预警模型对景区内可能发生的安全风险、资源破坏等事件进行预测和预警，设置不同的预警级别和预警方式，及时通知相关人员采取措施；
- c) 应急指挥：在景区发生突发事件时，实现应急指挥调度功能，包括救援力量的调配、物资的调度、应急预案的启动和执行等，通过视频会议、实时通讯等手段实现远程指挥和协同作战；
- d) 决策支持：通过对历史数据和实时数据的分析，为景区的规划、管理、运营等提供决策支持，如游客流量调控策略、设施维护计划制定、资源保护方案优化等；
- e) 信息发布：向游客和工作人员发布景区的相关信息，如景点介绍、活动通知、天气预警、安全提示等，信息发布渠道应包括景区官方网站、手机 APP、电子显示屏、广播系统等。

6 功能要求

6.1 系统构成

景区综合管理监测预警系统主要由水雨情监测系统、无线预警广播系统、监控系统、GNSS自动化监测预警系统构成。

6.2 水雨情监测系统

应对水位和雨量进行监测，具有雨量和水位数据智能采集功能，应具有长期固态存储和远距离传输功能。监测数据可通过GPRS/4G/5G，没运营商信号的时候可采用北斗卫星通信方式传输到中心预警平台。

6.3 无线预警广播系统

6.3.1 应在各种原始监测数据和历史数据分析对比的基础上，根据数据分析结果来决策预警信息，将预警信息及时准确地发送到现场进行广播预警。

6.3.2 能够通过 IP 话筒、麦克风等本地播发设备或电话、FM、DTMB、4G 等远程预警方式向需要预警区域的广播终端发布预警信息。

6.3.3 预警广播能够实时将接收到的预警信息进行广播预警, 有关单位，根据防御预案组织实施。

6.3.4 在通信畅通时，预警信息发布单位或责任人应能利用语音电话、手机 APP、手机短信等及时向下发布预警信息，各级广播终端根据接收的预警信息通过喇叭向外广播。

6.3.5 在无通信网络（或通信网络中断）时，根据当地预警设置配置的情况和危险情况，应能按照预案中事先确定的报警信号，利用监控视频 AI 识别预置预警信息向离线绑定的广播终端自动播发灾害可能威胁区域发送警报。

6.4 监控系统

6.4.1 应采用监控视频探头进行监测，可进行抓拍或移动物体监测，视频或图片通过设备传输到数据中心，视频可定制联动广播系统，一旦进入监控可视区域可触发监控视频开启，平时处于休眠状态。

6.4.2 监控选址应以能看到要监测点为准。

6.5 GNSS 自动化监测预警系统

6.5.1 滑坡体野外传感器采集系统应能收集野外现场的原始数据。

6.5.2 数据通讯系统应对数据监测和做出预警，使监测人员能快速分析信息。

6.5.3 供电等辅助支持系统应合理利用太阳能，并能稳定输出。

7 安全要求

7.1 网络安全

应符合GB/T 22239的要求，对系统网络进行安全防护。

7.2 数据安全

建立数据备份与恢复机制，定期对系统数据进行备份，确保数据在发生故障或灾难时能够快速恢复。

7.3 设备安全

7.3.1 自动化仪器设备应符合相关的国家标准、行业标准及 DZ/T 0460、DZ/T 0439 的相关要求。

7.3.2 对景区内的广播电视设备、物联网设备等进行安全管理，定期进行设备维护和升级，及时修复设备漏洞和安全隐患。

7.3.3 对设备的物理安全进行防护，防止设备被盗、损坏或恶意破坏。对重要设备，如服务器、核心网络设备等，应放置在专门的机房内，并采取防火、防水、防盗等安全措施。

7.4 应用安全

7.4.1 对系统应用进行安全开发，遵循安全编码规范，防止应用程序存在漏洞。

7.4.2 对应用系统的用户进行身份认证和授权管理，采用多因素认证方式，提高用户身份认证的安全性。

8 运维管理

8.1 运维制度

建立健全系统运维管理制度，包括设备维护制度、数据管理制度、安全管理制度、应急预案等。明确运维人员的职责和权限，规范运维工作流程和操作规范。

8.2 运维内容

8.2.1 设备运维

定期对系统设备进行巡检、维护和保养，及时更换损坏的设备部件，确保设备正常运行。对设备的运行状态进行实时监测，发现故障及时进行处理，并做好故障记录和分析。

8.2.2 数据运维

定期对系统数据进行备份、清理和优化，确保数据的可用性和性能。对数据的访问和使用进行审计和监控，防止数据泄露和滥用。

8.2.3 安全运维

定期对系统的网络安全、数据安全、设备安全 and 应用安全进行检查和评估，及时发现和修复安全漏洞。定期进行安全演练，提高系统的应急响应能力和安全防护水平。

8.3 人员培训

定期对运维人员进行技术培训和安全教育，提高运维人员的业务水平和安全意识。培训内容应包括系统的原理、功能、操作方法、维护技巧、安全知识等。
