ICS 27.140
CCS P 55

T/CS

团 体 标 准

T/CS 262—2026

水利工程信息化监测感知系统运行维护技术规范

Technical specification for operation and maintenance of information-based monitoring and sensing system for water conservancy projects

2026－02－27 发布 2026－02－27 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　缩略语 1
5　总体要求 2
6　硬件设备 2
7　软件 7
8　数据管理与维护 8
9　通信网络 9
10　安全保障 10
11　应急处置 12
12　维护记录与评估 13

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。

本文件由黄河水利委员会信息中心提出。

本文件由中国商品学会归口。

本文件起草单位：黄河水利委员会信息中心、河南黄河信息技术有限公司、山东黄河河务局德州黄河河务局、新源县水利局、新疆兴泽工程建设有限公司、新疆拓坤建设有限责任公司。

本文件主要起草人：于海泓、陈峰、薛冰峰、徐莉、王淮灵、章为、黄志、吴斌、王鹏、赵翼、丁卯、王龙、李安敏、顾冰、李欣、李萌、钱杰、李虹凡、祝娟、宁月美、刘恩辉。

水利工程信息化监测感知系统运行维护技术规范

1 范围

本文件规定了水利工程信息化监测感知系统（以下简称“系统”）运行维护的总体要求、硬件设备、软件、数据管理与维护、通信网络、安全保障、应急处置和维护记录与评估。

本文件适用于水利工程信息化监测感知系统的运行维护。

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 3411.1 大坝监测仪器 孔隙水压力计 第1部分：振弦式孔隙水压力计

GB/T 21978.2 降水量观测仪器 第2部分：翻斗式雨量传感器

GB/T 21978.3 降水量观测仪器 第3部分：虹吸式雨量计

SL 651 水文监测数据通信规约

SL 715 水利信息系统运行维护规范

SL/T 803 水利网络安全保护技术规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

信息化监测感知系统 information-based monitoring and sensing system

融合传感器技术、通信技术、物联网技术、大数据技术等，实现对水利工程运行状态、周边环境、水文情势等数据实时采集、传输、分析的综合系统。

3.2

数据采集设备 data acquisition device

接收传感器输出信号，并对信号进行调理、转换、采集、暂存的设备。

3.3

运行维护 operation and maintenance

为保障监测感知系统持续、稳定、可靠运行，对系统硬件设备、软件系统、网络通信、数据资源等进行的日常运维、例行运维、故障处置、应急处置等工作。

4 缩略语

下列缩略语适用于本文件。

AES：高级加密标准（Advanced Encryption Standard）

AP：接入点（Access Point）

ARP：地址解析协议（Address Resolution Protocol）

CPU：中央处理器（Central Processing Unit）
HTTPS：超文本传输协议安全版（Hyper Text Transfer Protocol Secure）
IP：网络协议（Internet Protocol）
IPS：入侵防御系统（Intrusion Prevention System）
Ping：互联网包探测器（Packet Internet Groper）
RAID：独立磁盘冗余阵列（Redundant Array of Independent Disks）
SMART：自我监测、分析与报告技术（Self-Monitoring, Analysis and Reporting Technology）
SQL：结构化查询语言（Structured Query Language）
SSD：固态硬盘（Solid State Drive）
VPN：虚拟专用网络（Virtual Private Network）

5 总体要求

5.1 系统由感知层、传输层、数据层和应用层组成，各层级的组成及要求如下：

a) 感知层由传感器、监控、数据采集等硬件设备组成，具有通过各类传感器、智能设备获取环境状态信息的功能；
b) 传输层由有线网络、无线网络及传输设备组成，具有根据数据的类型，选择最优传输路径的功能；
c) 数据层由存储和处理设备、数据库系统和数据处理软件组成，具有对传输层传来的海量原始数据进行清洗、存储、计算、分析的功能；
d) 应用层由各类业务软件组成，具有将数据层处理后的信息转化为具体的业务服务，直接面向用户或行业场景的功能。

5.2 系统运行维护应符合 SL 715 的规定，并遵循“预防为主、防治结合、及时响应、保障可靠”的原则。

5.3 系统运行维护的目标是保障系统长期稳定、可靠、高效运行，确保监测数据的准确性、完整性和及时性，为水利工程的安全运行、科学调度和精细化管理提供持续有效的数据支撑。

5.4 系统运行维护工作内容包括以下：

a) 日常运维：主要包括实时状态监控、现场简易巡检、数据日常管理、基础保障维护等；
b) 例行运维：根据设备类型与使用说明，制定明确的检修周期；每季度对监测平台软件、数据管理软件进行维护；每次例行维护后，详细记录维护内容、发现的问题、处理措施及设备状态，形成维护档案；
c) 故障处置：建立“分级排查”机制，第一时间定位故障点与故障原因；根据故障严重程度与影响范围，实施分级处置；故障修复后，24 h 内跟踪设备运行状态，确认故障无复发；
d) 应急处置：应建立完善的应急机制；当突发事件发生时，立即启动对应预案；突发事件结束后，分阶段开展恢复工作。

5.5 运维单位应配备具备相应技术能力的专业维护人员，并配置维护工具、检测设备及备品备件。

5.6 运维单位应建立岗位责任制、日常运维制度、例行运维制度、故障报告与处置制度、安全管理制度、技术档案管理制度等，并对制度执行情况进行检查与评估。

5.7 系统设备安装场所应具备良好的环境条件，机房温度应控制在 18 ℃～28 ℃，相对湿度应控制在 40%～60%；室外监测站点设备应具备防水、防潮、防尘、防腐蚀、防雷击、抗风、抗低温等防护能力。

5.8 监测站点应远离强电磁干扰、地质不稳定或易受洪水冲刷、淹没的位置。

6 硬件设备

6.1 传感器

6.1.1 运维对象

传感器运维对象包括水位计、渗压计、位移计、雨量计、水质传感器、流量计及其他类型传感器。

6.1.2 日常运维

每周至少进行1次日常运维，检查内容包括传感器外观是否完好、安装是否牢固、线缆连接是否可靠、防护措施是否完好；户外暴露的传感器还应检查是否有杂物遮挡、结冰等情况。

6.1.3 定期校准

传感器按以下规定进行校准：

a) 水位计：每 6 个月校准 1 次，当测量范围小于或等于 10 m 时，误差为±1 cm；当测量范围大于 10 m 时，误差为±0.1%FS；
b) 渗压计：应符合 GB/T 3411.1 的规定，每 12 个月校准 1 次，校准精度误差为±0.2%FS；
c) 位移计：每 12 个月校准 1 次，当量程不超过 100 mm 时，校准精度误差为±0.1mm；当量程大于 100 mm 时，校准精度误差为±0.1%FS；
d) 雨量计：符合 GB/T 21978.2、GB/T 21978.3 的规定，每 3 个月校准 1 次，校准精度误差为±2%；
e) 水质传感器：每 1 个月校准 1 次，pH 传感器校准误差为±0.1，溶解氧传感器校准误差为±0.2 mg/L，电导率传感器校准误差为±2%；其他水质传感器应符合相应产品标准的规定；
f) 流量计：管道式流量计每 6 个月校准 1 次，误差为±0.5%FS，明渠式流量计每 3 个月校准 1 次，误差为±1%FS，雷达测流计每 12 个月校准 1 次，误差为±2%FS；
g) 其他类型传感器：按产品技术说明书规定的周期与精度要求进行校准。

6.1.4 水位与流量的率定

6.1.4.1 一般要求

6.1.4.1.1 率定方法应适配测站断面水流特性及测验条件，且经过实践验证成熟可靠。

6.1.4.1.2 新设备正式投用前应完成首次率定，存量设备应按规定周期开展定期率定，遇特殊情况应启动应急率定。

6.1.4.1.3 率定过程应同步建立完整台账，记录设备信息、率定时间、人员、方法、数据及结果判定。

6.1.4.2 水位率定

6.1.4.2.1 在监测断面选取左、中、右 3 个代表性点位设置标准水位尺，同步读取自动水位计数据与人工尺读数据进行比对。

6.1.4.2.2 自动电子水位计每年至少开展 1 次率定。

6.1.4.2.3 水位变幅超过历年实测范围、设备维修后或数据出现持续偏差时，应立即补充率定。

6.1.4.3 流量率定

6.1.4.3.1 流速仪法适用于流速在仪器量程内、水深满足测点布置要求的情况。在断面布设垂线，每条垂线按水深比例设置测点，通过流速-面积法计算流量。

6.1.4.3.2 超声波法适用于含沙量较低、无大量漂浮物的情况。在两岸安装换能器，确保信号传输不受气泡干扰，结合断面面积计算流量。

6.1.4.3.3 流速仪每年标定 1 次，流量计每 2 年开展 1 次全面率定。

6.1.5 故障处置

当传感器出现故障时，按以下规定进行：

a) 无输出信号或信号异常：户外传感器应在 24 h 内到达现场排查，机房内传感器应在 8 h 内排查；

b) 测量精度超差：应在发现超差后 24 h 内重新校准，校准后仍超差的，应立即更换；

c) 物理损坏：应在发现损坏后 48 h 内更换。

注：确认故障后，若有备品备件，应在48 h内更换，无备品备件时应启动紧急采购流程，采购周期不超过7 d。

6.2 监控设备

6.2.1 运维对象

监控设备运维对象包括视频摄像头、音频采集设备、音频播放设备、监控主机、监控显示设备及配套的安装支架、电源适配器、传输线缆等附属设备。

6.2.2 日常运维

6.2.2.1 检查设备外观，查看摄像头、传感器外壳有无破损、变形，安装支架是否牢固、有无松动或倾斜，镜头、探头等关键部位是否存在遮挡、污渍或积水。

6.2.2.2 确认设备供电与连接，检查设备电源适配器、电源线有无老化、破损，插头接口是否插紧，传输线路有无断裂、脱落，设备指示灯是否处于正常工作状态。

6.2.2.3 核查实时运行数据，通过远程监控平台或本地终端，查看设备采集的数据是否连续、无异常跳变，视频监控画面是否清晰、无卡顿或黑屏，音频设备是否能正常收放音，确保设备初始运行状态无明显异常。

6.2.3 例行运维

6.2.3.1 对摄像头镜头、传感器探头进行除尘、除污，用专用清洁布擦拭表面杂质，清理设备周边杂草、杂物，避免环境因素影响设备运行。

6.2.3.2 检查设备接地线路是否牢固，测试接地电阻是否符合规定，预防雷击或漏电风险。

6.2.3.3 备份监控平台数据，清理冗余数据，检查软件运行日志，修复轻微软件漏洞。

6.2.3.4 对监控平台软件进行版本更新，根据业务需求优化功能模块，评估设备整体运行状况，制定老化设备的更换或升级计划。

6.2.4 故障处置与修复

6.2.4.1 通过远程查看设备运行日志、实时状态参数，结合现场运维人员反馈，判断故障类型：

a) 设备问题应确认具体故障部件；

b) 传输问题应排查线路是否断裂、网络设备是否故障；

c) 供电问题应检查电源适配器、配电箱开关是否正常。

6.2.4.2 故障处置与修复按以下规定进行：

a) 针对硬件故障，立即启用备用设备替换损坏设备，对损坏设备标记故障原因后送修；

b) 针对传输故障，修复或更换断裂线路，重启网络设备或重新配置网络参数，必要时联系运营商修复外部网络链路；

c) 针对软件故障，重启监控平台软件、恢复系统备份，或重新安装软件程序，清除软件缓存；

d) 针对供电故障，检查配电箱线路，更换损坏的电源部件，恢复稳定供电。故障验证与记录，故障修复后，通过远程平台和现场双重检查。

6.2.4.3 记录故障发生时间、地点、原因、处置过程及结果，纳入设备维护档案，同时分析故障规律，优化后续运维重点。

6.3 数据采集设备

6.3.1 运维对象

数据采集设备运维对象包括数据采集仪、信号调理设备、数据暂存设备及配套的电源适配器、信号线缆、接口模块等附属设备。

6.3.2 日常运维

6.3.2.1 每日通过远程监控或现场检查方式，查看数据采集设备运行状态、数据采集频率是否符合设定要求、与传感器及传输设备的通信是否正常。

6.3.2.2 每周现场检查 1 次设备供电电压、设备温度、线缆连接是否牢固。

6.3.3 例行运维

每3个月对数据采集设备进行1次例行运维，内容包括以下：

a) 清洁设备内部灰尘；
b) 检查设备接口有无氧化、松动，必要时进行除锈、加固处理；
c) 备份设备配置参数；
d) 测试设备数据采集精度。

6.3.4 故障处置

数据采集设备出现故障时，应按以下流程进行处置：

a) 远程排查：通过远程登录查看设备日志、配置参数，尝试重启、恢复出厂设置等操作，排查是否为软件或配置问题；
b) 现场处置：远程排查无法解决的，应及时到达现场，使用维护工具检测设备硬件，确认故障模块后，若有备品备件，应及时更换；无备品备件时，紧急采购周期不超过 5 d。

6.4 传输设备

6.4.1 运维对象

传输设备运维对象包括有线传输设备、无线传输设备及配套的传输线缆、天线、信号放大器等附属设备。

6.4.2 日常运维

6.4.2.1 每日通过网络监控平台查看传输设备运行状态，要求如下：

a) 带宽利用率：正常运行时不超过 70%，峰值时不超过 90%；
b) 丢包率：不超过 0.1%；
c) 时延：局域网内不超过 10 ms，广域网内 4G/5G 传输不超过 100 ms、卫星传输不超过 500 ms；
d) 4G/5G 模块信号强度：不低于-90 dBm；卫星终端信号强度：符合设备技术说明书要求。

6.4.2.2 每周现场检查 1 次传输设备外观、供电、线缆连接及天线安装情况。

6.4.3 例行运维

每6个月对传输设备进行1次例行运维，内容包括以下：

a) 清洁设备外壳及接口灰尘；
b) 检查设备固件版本，如有安全补丁或功能更新，应在测试环境验证后进行升级；
c) 测试传输链路稳定性：通过连续 24 h 传输测试，记录丢包率、时延等指标，确保符合日常运维要求；
d) 检查卫星天线对准精度。

6.4.4 故障处置

传输设备出现故障时，按以下规定进行处置：
a) 链路中断：排查是否为运营商网络故障，若为设备故障，现场处置人员应在 24 h 内到达现场，更换故障设备或模块，恢复链路通信；恢复后应进行 24 h 稳定性测试，确保指标正常；
b) 信号异常：4G/5G 模块信号弱时，检查天线安装位置，必要时调整天线方向或更换高增益天线；卫星终端信号异常时，重新校准天线对准精度，故障处置应在 48 h 内完成。

6.5 存储与处理设备

6.5.1 运维对象

存储与处理设备运维对象包括服务器、存储设备、数据处理终端及配套的电源模块、散热设备、连接线缆等附属设备。

6.5.2 日常运维

6.5.2.1 每日通过服务器监控软件查看存储和处理设备的运行状态，包括以下：
a) 服务器 CPU 利用率：正常运行时不超过 70%，峰值时不超过 90%；
b) 内存利用率：正常运行时不超过 70%，峰值时不超过 90%；
c) 硬盘使用率：不超过 80%，超过 80%时应及时清理冗余数据或扩容；
d) 硬盘健康状态：无坏道、SMART 报警信息。

6.5.2.2 每周现场检查 1 次设备供电、散热、线缆连接情况。

6.5.3 例行运维

每3个月对存储与处理设备进行1次例行运维，内容包括以下：
a) 备份数据库数据；
b) 清理服务器冗余日志文件、临时文件，优化操作系统和数据库性能；
c) 检查存储设备 RAID 状态，确保冗余功能正常；若有硬盘故障报警，应立即更换故障硬盘，重建 RAID 阵列；
d) 测试设备冗余功能，切换时间应不超过 30 s，切换后系统运行正常，数据无丢失。

6.5.4 故障处置

存储与处理设备出现故障时，按以下规定进行处置：
a) 服务器宕机：尝试立即重启，若无法重启，现场维护人员应在 2 h 内到达机房或协调机房运维人员排查故障，恢复服务器运行；
b) 恢复时间：硬件故障更换后不超过 4 h，软件故障修复后不超过 2 h；
c) 硬盘损坏：
   1) 若为 RAID 阵列中的硬盘，应在发现故障后 24 h 内更换故障硬盘，重建 RAID 阵列；
   2) 非 RAID 硬盘损坏时，若数据已备份，更换硬盘后恢复数据，恢复时间不超过 8 h；
   3) 若数据未备份，应联系专业数据恢复机构，数据恢复成功率应不低于 95%。

d) 数据库故障：无法访问时，首先排查数据库服务状态、连接参数，尝试重启数据库服务；若为数据损坏，使用备份数据恢复，恢复后数据完整性应为100%。

7 软件

7.1 系统软件

7.1.1 日常运维

每日检查操作系统、数据库系统、中间件的运行状态，包括以下：

a) 系统进程：无异常占用CPU、内存的进程；
b) 系统日志：无严重错误、致命错误日志信息；
c) 数据库连接数：不超过数据库最大连接数的80%；
d) 中间件服务：无宕机、重启异常情况，请求响应时间不超过3 s。

7.1.2 例行运维

每3个月进行1次系统软件例行运维，内容包括以下：

a) 操作系统补丁更新：筛选安全补丁，在测试环境验证兼容性后，对生产环境系统进行更新，更新后重启系统，确保服务正常；
b) 数据库优化：分析数据库性能缺陷，优化索引、表结构，清理历史冗余数据，数据库性能优化后，查询响应时间应较优化前提升不低于30%；
c) 中间件配置优化：根据业务负载调整中间件参数，测试中间件并发处理能力，确保并发用户数达到设计要求。

7.1.3 故障处置

系统软件出现故障时，处置要求如下：

a) 操作系统崩溃：使用系统备份镜像恢复，恢复时间不超过4 h；恢复后检查系统服务、软件兼容性，确保正常运行；
b) 数据库死锁：通过数据库管理工具排查死锁进程，终止死锁进程，恢复数据库正常运行，处置时间不超过30 min；同时分析死锁原因，优化SQL语句或业务逻辑，避免再次发生；
c) 中间件服务宕机：重启中间件服务，若重启无效，检查配置文件、日志信息，修复故障，处置时间不超过1 h；恢复后测试服务响应情况，确保正常。

7.2 应用软件

7.2.1 日常运维

每日通过应用系统监控界面或用户反馈，检查应用软件的运行状态，包括以下：

a) 功能可用性：所有功能模块均能正常使用，无功能失效情况；
b) 数据展示准确性：平台展示的监测数据与原始采集数据一致性不低于99.9%，无数据错位、缺失情况；
c) 预警功能有效性：模拟触发预警条件，预警信息应在10 min内发出，无漏报、误报；
d) 响应时间：页面加载时间不超过3 s，数据查询时间不超过5 s，多条件复杂查询时间不超过10 s。

7.2.2 例行运维

每6个月进行1次应用软件例行运维，内容包括以下：

a) 需求评估与优化：收集用户使用反馈，评估功能优化需求，对高频使用且体验不佳的功能进行优化，优化后用户操作效率提升不低于 20%；

b) 软件版本更新：若有新功能版本或 bug 修复版本，在测试环境完成功能测试和兼容性测试后，在业务低峰期对生产环境软件进行更新，更新过程中应做好数据备份，更新后进行 24 h 稳定性监控，确保无功能异常或性能下降；

c) 安全漏洞扫描与修复：使用专业安全扫描工具对应用软件进行漏洞扫描，扫描频率为每 3 个月 1 次，发现高危漏洞应在 24 h 内修复，中危漏洞应在 72 h 内修复，低危漏洞应在 1 周内制定修复计划并逐步落实。

7.2.3 故障处置

应用软件出现故障时，处置要求如下：

a) 功能失效：接收故障反馈后，技术人员应在 1 h 内复现故障，定位故障原因，并在 4 h 内提供临时解决方案，72 h 内完成彻底修复并上线验证；

b) 数据展示错误：排查是否为数据源错误，若为软件处理逻辑错误，应在 2 h 内修正处理算法，重新生成展示数据，确保数据准确性；若为界面渲染错误，应在 4 h 内修复前端代码，恢复正常展示；

c) 预警不触发：检查预警规则配置、数据输入链路，定位问题后 1 h 内调整配置或修复链路，修复后通过模拟数据测试预警功能，确保 10 min 内正常触发。

8 数据管理与维护

8.1 数据采集与接收

8.1.1 日常运维

每日检查数据采集频率、数据接收完整性，统计各监测点数据接收率，要求单监测点单日数据接收率不低于98%，全系统单日数据接收率不低于95%。

8.1.2 数据清洗维护

每周对采集数据进行1次清洗，清洗规则包括以下：

a) 剔除异常值：通过阈值判断、趋势分析识别异常数据，异常数据剔除后应标注原因；

b) 补全缺失值：对于短时间（低于 1 h）数据缺失，采用线性插值法补全；对于长时间（超过 1 h）数据缺失，标注“缺失”并关联故障记录，补全后数据应与原始数据区分存储，保留溯源痕迹。

8.1.3 故障处置

数据采集与接收异常时，处置要求如下：

a) 采集频率异常：排查数据采集设备配置参数、时钟同步状态，确认问题后 2 h 内调整配置或同步时钟，恢复正常采集频率；

b) 数据批量缺失：若为传输链路故障导致，优先修复链路；若为采集设备故障导致，修复设备后，通过设备本地缓存补传缺失数据，补传成功率不低于 90%，无法补传的应记录缺失时段及原因。

8.2 数据存储与备份

8.2.1 日常运维

每日检查数据存储状态，包括以下：

a) 存储介质健康度：硬盘、存储阵列无报错信息，存储读写速度符合设备标准；
b) 数据存储格式：符合 SL/T 803 规定的数据标准，元数据完整，无缺失或错误。

8.2.2 例行运维

数据备份应遵循“异地、多介质、定期验证”原则，具体要求如下：

a) 备份周期：实时监测数据每日进行增量备份，每月进行全量备份；历史统计数据每季度进行全量备份；
b) 备份介质：全量备份数据同时存储在本地硬盘阵列和异地存储服务器，增量备份数据存储在本地 SSD 和云存储；
c) 备份验证：每 3 个月对备份数据进行恢复测试，关键数据应全部恢复，一般数据随机抽取 10% 的备份文件进行恢复，恢复数据与原始数据一致性不低于 99.9%，全量备份恢复时间不超过 4 h，增量备份恢复时间不超过 1 h。

8.2.3 故障处置

数据存储与备份故障时，处置要求如下：

a) 存储介质损坏：若为 RAID 阵列中的介质，立即更换损坏介质并重建 RAID；若为非 RAID 介质，通过异地备份恢复数据，恢复时间不超过 8 h，确保数据无丢失；
b) 备份数据无法恢复：检查备份介质健康度、备份文件完整性，若为备份过程错误，重新执行备份操作；若为备份介质损坏，启用多介质备份中的其他副本，确保数据可恢复，应与原始数据进行对比确认。

8.3 数据共享与归档

8.3.1 数据共享维护

每月检查数据共享接口的可用性，确保接口响应时间不超过5 s，接口调用成功率不低于98%；对共享数据进行权限管控。

8.3.2 数据归档维护

数据归档应符合以下要求：

a) 实时监测原始数据：保存期限不低于 5 年；
b) 统计分析数据：保存期限不低于 10 年；
c) 工程安全相关数据：保存期限不低于工程设计使用年限；
d) 归档数据采用压缩存储，每年对归档数据进行 1 次完整性检查，确保无数据损坏或丢失，检查完成后生成归档数据完整性报告。

9 通信网络

9.1 局域网维护

9.1.1 日常运维

9.1.1.1 每日通过网络管理系统检查局域网设备运行状态，包括以下：

a) 设备负载：交换机端口带宽利用率不超过 70%，防火墙并发连接数不超过最大连接数的 80%；
b) 网络连通性：局域网内设备间 Ping 测试丢包率不超过 0.1%，时延不超过 5 ms；无线 AP 覆盖区域信号强度不低于-70 dBm，无明显信号盲区。

9.1.1.2 每周现场检查局域网线缆连接状态，无松动、老化、破损，光纤接头无灰尘或污渍。

9.1.2 例行运维

每6个月对局域网进行1次例行运维，内容包括以下：

a) 网络拓扑优化：根据设备接入数量变化调整网络拓扑结构，避免单点故障，优化后进行网络压力测试，确保网络稳定运行；
b) 配置备份与更新：备份交换机、防火墙配置文件，检查设备固件版本，如有安全更新或功能优化，在测试环境验证后进行升级，升级后测试网络功能无异常。

9.1.3 故障处置

局域网故障时，处置要求如下：

a) 网络中断：通过分层排查法定位故障点，物理层故障应在 2 h 内修复，设备故障应在 4 h 内更换或重启设备，恢复网络连通性；
b) 带宽异常：通过流量监控工具识别占用带宽的异常设备或应用，限制非必要流量，确保监测数据传输带宽优先，处置时间不超过 1 h，恢复后带宽利用率回归正常范围。

9.2 广域网维护

9.2.1 日常运维

9.2.1.1 每日检查广域网链路运行状态，包括以下：

a) 链路可用性：专线链路不低于 99.9%，4G/5G 链路不低于 99%，卫星链路不低于 98%；
b) 传输质量：广域网丢包率不超过 0.5%，专线时延不超过 200 ms、4G/5G 传输不超过 100 ms、卫星传输不超过 500 ms。

9.2.1.2 每周检查广域网设备配置参数，确保与运营商配置一致，无参数冲突。

9.2.2 例行运维

每3个月对广域网进行1次例行运维，内容包括以下：

a) 链路测试：采用测试工具进行链路带宽、吞吐量测试，确保实际带宽达到合同约定值的 90%以上；对卫星链路进行信噪比测试，信噪比不低于 5 dB；
b) 冗余链路验证：若配置多链路冗余，模拟主链路中断，测试备份链路自动切换功能，切换时间不超过 30 s，切换后数据传输正常，无丢失。

9.2.3 故障处置

广域网故障时，处置要求如下：

a) 链路中断：联系运营商确认是否为运营商网络故障，若为设备故障，24 h 内更换设备；若为运营商故障，跟踪运营商修复进度，修复后进行 24 h 链路稳定性测试，确保指标正常；
b) 传输质量下降：排查链路干扰因素，采取抗干扰措施；卫星链路传输质量下降时，检查天线对准精度或天气情况，必要时调整天线或等待天气好转，处置时间不超过 48 h。

10 安全保障

10.1 网络安全维护

10.1.1 日常运维

10.1.1.1 每日检查网络安全设备运行状态，包括以下：

a) 设备状态：无硬件故障报警，系统日志无高危安全事件记录；
b) 策略有效性：防火墙访问控制策略生效，IPS 规则库为最新版本。

10.1.1.2 每周检查局域网内设备 IP 地址分配情况，无非法 IP 地址接入，无 ARP 欺骗攻击迹象。

10.1.2 例行运维

每3个月进行1次网络安全维护，内容包括以下：

a) 安全漏洞扫描：对网络设备、服务器进行全端口漏洞扫描，发现高危漏洞 24 h 内修复，中危漏洞 72 h 内修复，扫描结果生成漏洞报告并归档；
b) 渗透测试：邀请第三方安全机构对系统进行渗透测试，模拟黑客攻击手段，发现安全隐患后制定整改方案，整改完成率 100%。

10.1.3 故障处置

网络安全事件时，处置要求如下：

a) 攻击处置：发现攻击后立即启动应急预案，断开受攻击设备网络连接，收集攻击日志，1 h 内上报主管部门，24 h 内完成攻击溯源，修复漏洞并恢复系统运行；
b) 数据泄露：若发生监测数据泄露，立即停止数据共享服务，排查泄露途径，2 h 内采取补救措施，24 h 内提交数据泄露事件报告，评估泄露影响并制定预防措施。

10.2 数据安全维护

10.2.1 日常运维

10.2.1.1 每日检查数据加密状态，包括以下：

a) 传输加密：监测数据通过 HTTPS、VPN 或符合 SL 651 规定的专用加密协议传输，无明文传输情况；
b) 存储加密：敏感数据采用 AES-256 加密算法存储，加密密钥定期更换，密钥存储在专用密钥管理设备中。

10.2.1.2 每周检查数据访问日志，无未授权访问记录，访问日志保存期限不低于 6 个月。

10.2.2 例行运维

每6个月进行1次数据安全维护，内容包括以下：

a) 加密算法验证：测试数据加密/解密功能有效性，确保加密后数据无法被非法破解，解密后数据与原始数据一致性 100%；
b) 访问权限审计：对所有数据访问用户权限进行审计，删除过期权限、冗余权限，确保权限与岗位职责匹配，审计结果生成权限审计报告并归档。

10.2.3 故障处置

数据安全故障时，处置要求如下：

a) 密钥丢失：启用密钥备份，2 h 内恢复密钥，若备份密钥也丢失，立即重新生成新密钥并对所有加密数据重新加密，加密完成时间不超过 24 h，确保数据可正常访问；

b) 数据篡改：通过数据校验码比对识别篡改数据，从备份中恢复原始数据，排查篡改原因，修复漏洞并加强访问控制，防止数据再次被篡改。

10.3 终端安全维护

10.3.1 日常运维

每日检查维护终端安全状态，包括以下：

a) 杀毒软件：安装正版杀毒软件，病毒库更新时间距当前不超过 1 d，实时防护功能开启，无病毒或恶意软件感染记录；

b) 系统安全：操作系统补丁为最新版本，开启防火墙功能，禁用不必要的端口。

10.3.2 例行运维

每3个月对维护终端进行1次安全维护，内容包括以下：

a) 全盘杀毒：对终端进行全盘病毒扫描，清除恶意软件或病毒，扫描完成后生成杀毒报告；

b) 系统清理：清理终端冗余文件、临时文件，检查是否存在非法软件，发现后立即卸载并记录。

10.3.3 故障处置

终端安全故障时，处置要求如下：

a) 病毒感染：立即断开终端网络连接，启动杀毒软件进行全盘扫描和清除，清除完成后重启终端并测试网络连接，确保无残留病毒，处置时间不超过 2 h；

b) 系统入侵：重装操作系统，重新配置安全策略，恢复终端数据，恢复时间不超过 4 h，同时检查其他终端是否存在相同入侵风险，防止扩散。

11 应急处置

11.1 应急预案制定

11.1.1 维护单位应制定系统应急处置预案，内容包括：

a) 应急组织架构：明确应急指挥人员、技术处置人员、联络人员职责；

b) 应急响应流程：分为预警、启动、处置、恢复、总结 5 个阶段，每个阶段明确操作步骤、时间要求；

c) 应急保障措施：配备应急设备、应急通信工具、应急电源，每月 1 次检查应急设备状态。

11.1.2 应急预案应每年评审 1 次，根据实际运行情况进行修订，修订后组织全员培训。

11.2 应急响应分级

根据故障影响范围、严重程度，将应急响应分为Ⅰ级、Ⅱ级、Ⅲ级、Ⅳ级4个等级，具体划分要求如下：

a) Ⅰ级响应：全系统瘫痪，影响工程监测感知系统正常运行，应启动最高级应急处置；

b) Ⅱ级响应：局部系统故障，对工程监测精度或效率产生较大影响；

c) Ⅲ级响应：单个监测区域或功能模块故障，对整体系统运行影响有限，可通过替代方案临时保障监测需求；

d) Ⅳ级响应：单个监测点或设备故障，不影响其他监测功能，修复周期较短。

11.3 应急处置流程

11.3.1 预警

通过系统监控平台、现场运维或用户反馈发现故障后，维护人员应在10 min内完成故障初步判断，明确故障类型、影响范围及严重程度，根据应急响应分级标准确定响应等级，并通过应急联络群向应急指挥人员报告，报告内容包括故障时间、地点、现象、初步判断结果及建议响应等级。

11.3.2 启动

应急指挥人员接到报告后，15 min内审核响应等级，下达应急启动指令：

a) Ⅰ级响应：立即通知全体应急人员到岗，协调外部技术支持，启动应急备用系统；
b) Ⅱ级响应：通知核心应急人员到岗，启动局部备用方案；
c) Ⅲ级/Ⅳ级响应：安排责任维护人员到场处置，无需全员集结。

11.3.3 处置

技术处置人员根据故障类型执行以下对应处置方案：

a) 硬件故障：优先更换备用设备，无备用设备时紧急调拨，更换后立即调试，确保监测感知系统恢复正常；
b) 软件故障：Ⅰ/Ⅱ级响应时优先回退至稳定版本，同时排查故障原因；Ⅲ/Ⅳ级响应时可现场修复，修复后测试功能完整性；
c) 网络故障：Ⅰ/Ⅱ级响应时立即切换备用链路，Ⅲ/Ⅳ级响应时现场排查链路断点，修复线缆或设备；
d) 数据故障：若发生数据丢失或篡改，立即从异地备份恢复数据，恢复后验证数据完整性。

11.3.4 恢复

11.3.4.1 故障处置完成后，对系统进行稳定性测试：

a) Ⅰ/Ⅱ级响应：持续监测 24 h，确保监测数据接收率不低于 95%、软件功能无异常、网络传输稳定，测试通过后正式恢复系统运行，同时关闭备用系统；
b) Ⅲ/Ⅳ级响应：持续监测 8 h，确认故障模块运行正常，无故障复现迹象，即可恢复正常维护流程。

11.3.4.2 恢复运行后，技术处置人员向应急指挥人员提交恢复报告，说明处置结果、系统当前状态及后续观察建议。

11.3.5 总结

应急响应结束后7 d内，应急指挥人员组织召开总结会议，分析故障原因、评估处置效果、梳理存在问题，形成应急处置总结报告，并根据报告内容修订应急预案或优化维护制度。

12 维护记录与评估

12.1 维护记录管理

12.1.1 记录内容

维护人员应实时记录各项维护工作，记录内容应完整、准确、可追溯，具体包括以下：

a) 日常运维记录：日期、运维人员、运维设备、运行状态、发现问题及处理建议，若未发现问题应标注“正常”；

b) 例行运维记录：维护日期、维护类型、维护设备清单、维护步骤、使用工具/耗材、维护结果、异常情况及处理方式；
c) 故障处置记录：故障发生时间、发现人、故障现象、定位过程、处置措施、处置时间、恢复时间、故障原因分析、预防措施；
d) 应急处置记录：响应等级、启动时间、参与人员、处置过程、备用设备使用情况、恢复时间、总结报告编号；
e) 数据管理记录：数据采集率统计、数据清洗日志、备份/恢复记录、归档数据清单。

12.1.2 记录形式与存储

12.1.2.1 记录形式

采用电子记录为主，纸质记录为辅，电子记录应设置修改权限。

12.1.2.2 存储要求

电子记录存储在本地服务器和异地备份服务器，纸质记录归档至专用档案柜，分类存放，存储环境应干燥、避光、防虫蛀，保存期限不低于5年。

12.1.3 记录检查

维护负责人每月对维护记录进行1次检查，检查内容包括记录完整性、准确性、及时性，发现问题及时督促整改，检查结果形成维护记录检查报告，并与维护记录一并归档。

12.2 维护效果评估

12.2.1 维护效果评估分为月度评估、年度评估，年度评估可结合水利工程年度检修工作同步开展。
12.2.2 月度评估由维护单位内部组织；年度评估可邀请第三方机构参与，确保评估客观性。
12.2.3 评估流程如下：
a) 评估小组收集当月、年度维护记录、系统运行日志、故障报告、应急处置总结等数据，确保数据真实有效；
b) 根据收集的数据计算各项评估指标，对比标准要求，识别未达标指标；
c) 对未达标指标进行深入分析，明确原因；
d) 针对原因制定可落地的改进措施，明确责任人和完成时限；
e) 形成维护效果评估报告，内容包括评估概况、指标计算结果、原因分析、改进措施及下一步工作计划，报告应经评估主体签字确认后归档。