

探析气象部门计算机网络系统运行管理及维护措施

吴秀娟¹ 吴秀艳²

1. 济南市气象局 山东 济南 250000

2. 济南市军粮供应有限公司 山东 济南 250000

摘要: 气象部门计算机网络系统涵盖硬件、软件、网络等多层面, 承担数据采集、预报、发布等关键职能, 具有数据量大、实时性要求高、覆盖范围广等特点。当前系统运行管理存在硬件老化、软件兼容性差、网络带宽瓶颈、安全风险突出、人员技能不足等问题。本文从硬件维护、软件升级、网络安全、动态监控、人员与制度保障等方面提出针对性措施, 以提升系统运行稳定性与服务效能。

关键词: 气象部门; 计算机网络系统; 运行管理; 维护措施

引言: 在气候变化愈发显著、气象灾害频繁发生的当下, 气象信息对于防灾减灾、保障生产生活的重要性不言而喻。气象部门计算机网络系统作为气象数据采集、处理、分析以及发布的核心支撑, 其稳定运行至关重要。然而, 该系统面临着硬件老化、软件兼容性不佳、网络安全威胁等诸多挑战。因此, 深入探析其运行管理及维护措施, 对提升气象服务质量和保障社会稳定发展意义重大。

1 气象部门计算机网络系统概述

1.1 系统组成与功能

(1) 硬件架构: 核心包含服务器集群, 承担海量气象数据存储与运算任务, 可实现多节点并行处理; 传感器网络覆盖广泛, 涵盖地面温湿度传感器、高空探空仪、雷达设备等, 实时捕捉大气各类参数; 通信设备以光纤、卫星通信为主, 保障数据在不同区域间高效传输, 确保偏远站点数据不中断。(2) 软件系统: 数据采集平台具备多源数据接入能力, 可整合传感器、卫星、雷达等各类数据, 同时完成数据清洗与格式标准化; 预报模型集成数值天气预报、统计预报等多种算法, 能模拟大气运动趋势, 支撑短期、中期、长期预报; 信息发布系统支持多渠道输出, 可通过官网、APP、短信、预警终端等, 将气象信息传递给用户。(3) 网络拓扑结构: 采用分级分层设计, 国家级节点作为核心, 负责全国气象数据汇总、模型运算与决策指挥; 省级节点承接国家级指令, 处理区域内数据并进行区域预报; 市级节点聚焦本地气象服务, 细化预报产品; 站点级节点则侧重数据采集与基层信息反馈, 形成自上而下、协同联动的网络体系。

1.2 系统特点

(1) 数据量大且类型复杂: 每日需处理TB级数据,

涵盖文本型的观测记录、图像型的卫星云图、视频型的雷达回波动态影像等, 数据格式多样, 需专用技术进行存储与分析。(2) 实时性要求高: 数据更新需达到分钟级, 从数据采集、传输到处理、发布, 每个环节都需高效衔接, 确保气象预报、灾害预警能及时推送, 为防灾减灾争取时间。(3) 覆盖范围广: 监测范围从地面延伸至高空, 涵盖城市、乡村、山区、海洋等不同区域, 通过布设各类监测设备, 构建全方位、立体化的气象监测网络, 确保无监测盲区^[1]。

1.3 典型应用场景

(1) 气象灾害预警系统: 通过实时分析气象数据, 当监测到台风、暴雨、暴雪、寒潮等灾害性天气时, 能快速生成预警信息, 明确灾害影响范围、强度与持续时间, 及时向政府部门、企业及公众发布, 指导防灾避险工作, 降低灾害损失。(2) 气候监测与预测模型: 长期监测气温、降水、风速等气候要素变化, 构建气候预测模型, 可预测月、季、年尺度的气候趋势, 为农业生产、水资源管理、能源调度等提供科学依据, 助力应对气候变化。(3) 公众气象服务信息发布: 针对公众日常需求, 提供精细化气象服务, 如未来24小时逐小时预报、生活指数(穿衣、出行、防晒等)预报, 通过多种便捷渠道实时发布, 满足公众出行、生活安排等需求, 提升生活质量。

2 气象部门计算机网络系统运行管理现状分析

2.1 现有管理框架

(1) 分级管理制度: 采用国家-省-市三级联动模式, 国家级管理部门统筹整体系统规划、核心资源调配与跨区域协调, 负责制定全国统一的管理规范与技术标准; 省级管理部门聚焦区域内系统运维, 承接国家级任务并向下传导, 同时处理省内特殊气象场景的系统适配

需求；市级管理部门则侧重本地设备维护、数据初步核验与基层服务对接，形成“上层统筹、中层执行、基层落地”的分级管理体系，保障系统整体运行有序^[2]。

(2) 标准化流程：引入ISO20000IT服务管理标准，构建覆盖系统全生命周期的标准化流程。从设备采购、安装调试，到日常运维、故障排查，再到系统升级、退役更替，均制定明确操作规范；数据管理环节严格遵循数据采集、清洗、存储、共享的标准化流程，确保数据质量与安全性；同时建立标准化的服务响应机制，明确故障处理时限与服务评价指标。

2.2 现存问题

(1) 硬件层面：部分偏远地区与老旧站点设备老化严重，服役超10年的传感器、服务器占比达30%以上，数据采集精度与运算效率下降；区域性覆盖不足，高海拔山区、偏远海岛仍存在监测盲区，难以捕捉局部小尺度灾害天气；且多数硬件缺乏抗灾设计，台风、暴雨等极端天气易导致设备损坏，抗灾能力弱，影响系统连续运行。(2) 软件层面：不同时期建设的软件系统兼容性差，省级与市级部分预报模型、数据平台无法无缝对接，数据共享需人工转换格式；软件更新滞后于业务需求，新的气象观测技术与预报算法难以快速集成，导致系统功能跟不上气象服务精细化要求；同时软件漏洞修复不及时，平均漏洞修复周期超15天，增加系统运行风险。(3) 网络层面：部分市级与站点级网络存在带宽瓶颈，高峰时段（如灾害天气监测期）数据传输速率下降50%以上；偏远地区依赖卫星通信，受信号干扰影响，数据传输延迟可达分钟级，影响实时预报；跨部门协作中，气象系统与应急、农业等部门网络接口不统一，数据共享效率低，协作困难。(4) 安全层面：外部安全威胁频发，每年遭遇DDoS攻击超千次，勒索软件攻击案例逐年增加，部分基层站点因防护措施不足，曾出现数据被加密、系统瘫痪的情况；内部安全风险同样突出，约20%的故障由工作人员误操作引发，如误删关键数据、违规接入外部设备，内部安全管控存在漏洞。(5) 人员层面：基层运维人员专业技能不足，仅40%人员具备网络安全、大数据运维等复合型技能，难以应对复杂系统故障；应急响应机制不完善，多数市级部门未建立24小时应急团队，灾害天气导致系统故障时，平均响应时间超2小时，延误气象服务与灾害预警工作。

3 气象部门计算机网络系统运行管理及维护措施

3.1 硬件维护优化

(1) 定期巡检与预防性更换老化设备：制定“季度巡检+年度评估”机制，组织专业团队对服务器集群、传

感器、通信设备等进行全面检测，重点排查设备运行温度、性能衰减、部件损耗等问题；建立设备生命周期台账，对服役超8年、故障率超20%的老化设备，提前纳入更换计划，优先保障国家级核心节点与灾害高发区域设备更新，避免因硬件故障导致系统中断。(2) 部署冗余备份系统：核心网络节点采用双链路设计，主链路选用光纤通信，备用链路搭配卫星或4G/5G无线通信，当主链路中断时，自动切换至备用链路，保障数据传输不中断；关键设备（如核心服务器、数据存储设备）配备UPS不间断电源，支持断电后持续供电2-4小时，同时在省级以上节点建设备用机房，实现核心数据与业务的异地容灾备份^[3]。(3) 强化野外站点设备的抗灾设计：针对野外站点易受极端天气影响的问题，传感器外壳采用防水等级IP67以上、抗腐蚀的材质，内部加装防雷模块，避免雷击损坏电路；设备安装支架采用高强度钢材，能抵御12级以上大风，同时在站点周边搭建防风障、排水沟，减少暴雨、暴雪对设备的冲击，提升野外设备的抗灾能力。

3.2 软件系统升级

(1) 采用模块化架构提升系统可扩展性：对现有数据采集平台、预报模型等软件进行模块化重构，将核心功能拆分为独立模块（如数据接入模块、运算模块、输出模块），新功能可通过新增模块快速集成，无需重构整个系统；同时统一模块接口标准，实现国家级、省级、市级软件系统的模块互通，解决系统兼容性问题。(2) 建立自动化更新与补丁管理机制：搭建中央化软件管理平台，对各级节点软件进行统一监控，当出现新版本或安全补丁时，自动推送更新通知，支持批量部署与断点续更；设置更新审核机制，先在测试环境验证更新稳定性，再逐步在生产环境推广，避免更新引发系统故障。(3) 引入AI技术优化数据处理效率：在数据预处理环节，应用AI智能压缩算法，对冗余度高的卫星云图、雷达数据进行无损压缩，减少数据存储与传输压力；采用AI去噪算法，去除传感器采集数据中的干扰信号，提升数据准确性；在预报模型中融入AI深度学习技术，通过分析历史气象数据，优化预报参数，提高短期预报精度^[4]。

3.3 网络安全强化

(1) 构建分层防御体系：在网络边界部署下一代防火墙，拦截非法访问与恶意流量；在服务器端安装入侵检测与防御系统（IDS/IPS），实时监测异常操作与攻击行为；对敏感气象数据（如预报模型参数、灾害预警原始数据）采用AES-256加密算法，实现数据传输与存储全程加密，防止数据泄露。(2) 定期开展渗透测试与漏洞

扫描：每季度组织专业安全团队进行渗透测试，模拟黑客攻击手段，排查系统潜在安全漏洞；利用自动化漏洞扫描工具，对网络设备、服务器、软件系统进行每日扫描，形成漏洞清单并按风险等级排序，低风险漏洞7日内修复，高风险漏洞24小时内紧急处置。（3）加强员工安全意识培训与权限分级管理：每月开展安全培训，内容涵盖DDoS攻击防范、勒索软件应急处理、内部操作规范等，通过案例讲解与模拟演练提升员工安全意识；实施最小权限原则，根据岗位需求分配系统操作权限，普通运维人员仅具备基础操作权限，核心数据修改权限仅限少数管理员，同时开启操作日志审计功能，追溯异常操作。

3.4 动态监控与故障预警

（1）部署全维度网络性能监测工具：采用SNMP协议对网络设备（路由器、交换机）进行实时监控，采集带宽利用率、数据包丢失率等指标；通过NetFlow分析技术，追踪数据传输路径，定位传输瓶颈；在服务器与软件系统中部署监控代理，实时采集CPU使用率、内存占用、服务响应时间等数据，所有监测数据统一汇总至中央监控平台，实现可视化展示。（2）建立基于大数据的故障预测模型：利用大数据分析技术，对历史故障数据（故障类型、发生时间、触发条件）进行挖掘，识别故障发生规律，构建故障预测模型；当监控数据达到预设阈值（如带宽利用率超90%、服务器CPU占用超85%）时，模型自动生成预警信息，通过短信、邮件推送至运维人员，实现故障提前预判^[5]。（3）制定应急预案并定期演练：针对断电、断网、系统瘫痪等常见故障场景，编制详细应急预案，明确应急响应流程、责任分工与资源调配方案；每半年组织一次应急演练，模拟极端天气导致的网络中断、勒索软件攻击等场景，检验应急预案可行性，优化应急处置流程，将故障恢复时间缩短至1小时以内。

3.5 人员与制度保障

（1）组建专业化运维团队并定期技能培训：面向全国气象系统选拔网络运维、安全防护、AI技术等领域专业人才，组建国家级核心运维团队，省级、市级配备专

职运维人员；建立“年度培训+季度考核”机制，培训内容涵盖新技术（如5G、AI在气象系统的应用）、应急处置技能等，考核不合格者需重新培训，确保团队专业能力满足系统运维需求。（2）完善运维管理制度：在ISO20000标准基础上，细化变更管理流程，系统升级、设备更换等变更需经过申请、评估、审批、实施、验收五个环节，避免无序变更引发风险；建立问题管理流程，对故障问题进行分类归档，分析根本原因并制定预防措施，形成“发现问题-解决问题-预防问题”的闭环管理；同时明确运维人员岗位职责与考核指标，将系统故障率、故障恢复时间纳入绩效考核。（3）推动跨部门协作机制：与通信运营商签订长期合作协议，保障气象专用网络带宽扩容需求，当出现网络故障时，运营商需在1小时内响应、4小时内修复；与电力部门建立联动机制，优先保障国家级、省级气象节点供电稳定，提前获取停电通知，做好应急供电准备。

结束语

气象部门计算机网络系统的高效运行，是精准气象服务的重要基石。通过对硬件维护优化、软件系统升级、网络安全强化、动态监控预警以及人员与制度保障等多方面举措的深入探讨与实施，能够有效应对当前系统运行管理中存在的各类问题。未来，还需持续关注技术发展动态，不断优化管理与维护策略，以保障系统稳定，为社会提供更优质、可靠的气象服务。

参考文献

- [1]张旭阳,张元龙,贾思阳,等.气象部门计算机网络系统运行管理和维护探讨[J].电脑知识与技术,2021(8):25-26.
- [2]郭卫亮.计算机网络在气象业务中的应用及病毒防御措施[J].信息周刊,2020(40):51-52.
- [3]罗铭浩.计算机网络安全防护措施研究[J].信息与电脑,2020,32(5):29-31.
- [4]王乐.气象部门计算机网络系统运行管理及维护[J].中国科技信息,2020(09):77-79.
- [5]吴劲松.气象部门计算机网络系统运行管理和维护探讨[J].神州,2020(10):18-20.