工程与管理科学
Engineering and Management Science
第 7 卷◆第 11 期◆版本 1.0◆2025 年
文章类型：论文|刊号（ISSN）：2705-0637(P) / 2705-0645(O)

新一代集中监控系统网络安全防护策略分析

陈柳叶　崔玉璐　白昀　王鹏
国网冀北电力有限公司秦皇岛供电公司　河北秦皇岛　066000

DOI：10.12238/ems.v7i11.16086

［**摘　要**］随着信息技术的快速发展，新一代集中监控系统在保障公共安全、提高管理效率方面发挥着重要作用。然而，系统的网络安全风险也日益凸显。为了有效应对这些风险，新一代集中监控系统需要采取“主动防御+动态防护”的策略框架，构建纵深防御体系，并遵循安全合规与标准化要求。本文分析了新一代集中监控系统的网络安全防护策略，包括身份认证与访问控制机制的强化、数据加密与安全传输技术的应用、网络隔离与分区管理策略、入侵检测与威胁感知技术的应用、安全日志与行为审计管理以及应急响应与容灾备份机制的建立。

［**关键词**］网络安全；集中监控系统；防护策略；身份认证；数据加密

引言

数字化时代背景下，新一代集中监控系统是维护社会安全的主要技术手段，网络安全防护能力的强弱直接影响着公共安全与社会稳定。在网络攻击手段日益更新与复杂化的今天，集中监控系统遇到了空前的网络安全问题。所以，对目前集中监控系统网络安全风险进行深入剖析，提出行之有效的防护策略对提高系统安全防护水平，确保数据安全及系统稳定运行有着十分重要的作用。

一、集中监控系统的网络安全风险分析

（一）系统架构的复杂性与潜在漏洞

新一代集中监控系统一般包括数据采集层、传输层、存储层以及应用层，覆盖了监控终端、网络设备、服务器以及管理平台的各种软硬件部分。系统架构的复杂性以及各层间接口与协议的多样性使潜在漏洞极易为攻击者所利用。比如设备固件更新不够及时会造成安全隐患、界面未经加固会被用来非法访问、第三方软件集成会引入未知漏洞等。另外，系统功能扩展和模块增加通常伴随着权限管理、通信协议以及数据流路径等方面的改变，若没有统一的安全设计就可能导致漏洞链。

（二）常见攻击方式

集中监控系统所面对的网络攻击手段是多种多样。恶意软件在终端或者服务器上的植入会盗用数据或者损坏系统功能；DDoS 攻击以海量流量轰炸的方式瘫痪了监控服务并影响实时监控和报警响应；越权访问攻击利用权限管理的漏洞来获得更高的操作权限，并对配置或数据进行篡改。另外，钓鱼攻击、漏洞利用以及供应链攻击等都是普遍存在的威胁，这类手段通常具有隐蔽性和破坏性的特点。当系统受到攻击时，不但会引起监控数据的损失，而且会导致指挥调度的失败，从而给企业或者公共安全带来直接的威胁。

（三）内部人员风险与管理漏洞

内部人员风险来自管理员、运维人员、使用者等方面的不正当操作或者恶意行为。权限配置不合理、操作规程不规范及行为监控的缺失等因素，会造成内部数据泄露、设备误操作乃至系统恶意篡改等问题。同时，管理漏洞主要表现为缺少定期审计、密码策略宽松和日志追踪不到位，放大了企业内部风险。特别是集中监控系统、运维人员一般都具有广泛的权限，如果出现管理漏洞或者内部控制松懈，就会引发严重的安全事件，对系统稳定性和数据安全产生威胁。

（四）数据传输与存储中的安全隐患

集中监控系统的数据采集、传输、存储等环节存在着诸多安全隐患。网络传输中的数据可能会受到窃听或者篡改，特别是跨部门或者跨区域的传输会存在较大的风险；存储环节如果缺少加密、备份、访问控制等功能，还易造成数据的泄露、丢失或者篡改。另外，日志信息、配置文件以及历史录像这些敏感数据如果管理不到位，会提高攻击者使用的概率。

二、新一代集中监控系统网络安全防护总体思路

（一）“主动防御+动态防护”的策略框架

新一代的集中监控系统的安全防护应以“主动防御+动态防护”作为其核心战略。主动防御从漏洞扫描、入侵检测、威胁情报以及安全配置加固等方面，对潜在的攻击进行预先识别与屏蔽；动态防护系统利用实时监测、行为分析和流量异常检测等多种手段，对系统的运行状况进行持续的评估，

从而能够迅速地应对新出现的威胁。另外，主动和动态防护相结合，能够实现威胁预警，快速定位以及自动屏蔽攻击链等功能，构成了闭环安全管理体系，增强了系统整体的安全性和稳定性。

（二）纵深防御体系构建思路

纵深防御突出了不同安全层次上多重防护屏障的设置，主要表现为终端安全、网络安全、应用安全及数据安全。采用分层防护的方法，可以使攻击风险层层消减，甚至在某个环节被入侵时，系统的整体不失效。就集中监控系统而言，可以通过防火墙、入侵防御系统、访问控制和数据加密等多种方式构成纵深防御网络。同时通过安全策略统一管理、日志集中分析以及定期演练等手段，可以增强系统对复杂攻击行为的抵抗能力，全方位覆盖安全防护。

（三）安全合规与标准化要求

新一代集中监控系统的建设与运营必须符合国家网络安全法律法规和行业标准，如等保 2.0、ISO27001 标准。安全合规既是法律要求，又有利于规范系统设计、运维流程以及应急响应机制。标准化要求涉及权限管理、数据保护、审计日志、风险评估及应急响应，有助于构建可量化、安全可控管理体系。另外，定期的安全评估与整改可以保证系统不断达到合规的标准，促进整体安全水平的提升。

三、新一代集中监控系统网络安全防护策略分析

（一）身份认证与访问控制机制强化

身份认证与访问控制作为集中监控系统安全保护的第一步，是预防未授权访问与内部滥用行为的核心举措。在身份认证方面，传统的用户名密码认证已难以应对现代攻击威胁，必须结合多因素认证（MFA）、生物特征识别（例如指纹，虹膜或者面部识别）、一次性动态口令（OTP）和硬件令牌实现了身份验证多重保证。多因素认证可以显著减少凭证泄露的危害，特别适用于远程访问、跨部门管理等场景。同时，可通过统一身份管理系统（IDM）和单点登录（SSO）对系统内的所有用户进行集中管理，确保用户生命周期全程可控，从注册、授权、变更到注销都具备记录和审计能力。在访问控制机制上，要按照最小权限原则对用户、角色、设备等权限进行细化，保证每一个账号都能获取到自己责任内的信息与功能。角色基于访问控制（RBAC）和属性访问控制（ABAC）是当前的主流方法，可以根据用户身份、工作岗位、操作时间、对访问终端及其他要素的权限进行动态调整，达到灵活授权、精确控制的目的。另外，对于高敏感的操作，例如系统配置变更、录像导出和告警策略修改，要建立二次认证或者审批流程以提高操作的可控性。

（二）数据加密与安全传输技术应用

就集中监控系统而言，数据安全问题是其可靠工作的核心问题。监控系统中涉及的敏感信息非常多，所以数据加密与安全传输技术运用起来就显得格外关键。静态数据可采用对称加密（如 AES）、非对称加密（如 RSA）以及混合加密模式来保护存储安全；对于关键的配置文件及日志信息也可以采用磁盘加密与数据库字段加密相结合的方式，以保证系统受侵害或者物理设备失窃后的数据不能解密使用。数据传输环节中，安全通信协议为防范窃听、篡改及重放等攻击提供了重要保证[1]。可以采用 TLS/SSL、IPsec VPN、HTTPS 协议进行端到端的加密，确保数据在局域网、广域网和云端传输安全。同时对于跨部门、跨区域或者远距离接入的场景，要使用加密的隧道或者特殊的安全通道，防止传输链路上的数据被拦截。为了进一步加强安全性，可以将网络防火墙、入侵防御设备与数据完整性校验机制相结合，从而达到多层防护的目的。密钥管理对于确保加密效果同样重要，它包括密钥的产生、发布、更新和销毁等环节，在整个过程中必须对访问权限进行严格把控，对密钥进行定期轮换，对操作日志进行记录，防止密钥泄露或者误用。

（三）网络隔离与分区管理策略

就集中监控系统而言，一般涉及到前端采集终端、传输网络、存储服务器、管理平台以及外部接入的诸多环节。采用物理隔离或者逻辑隔离的方法把不同功能模块或者安全等级的区域分割成独立的网络，可把潜在的威胁限制在某一区域内。举例来说，前端的数据采集设备、核心的管理服务器以及外部的访问路径都被划分为不同的区域，而这些区域之间则是通过防火墙和访问控制列表（ACL）来实现的、安全网关或者 VPN 连接以及制定严格的接入策略来约束非授权接入以及跨区通信[2]。分区管理既可以限制攻击的蔓延，又可以在每个分区采取差异化的安全策略。比如关键存储区可启用较高层次的入侵防护，深度包检测以及流量审查等功能，外部接入区主要保护 DDoS、端口扫描以及弱口令攻击等。将网络安全监控与日志分析相结合，能够对跨区访问的异常情况进行实时监控，并迅速检测出可能存在的风险。另外，采用分区管理也可以促进运维管理效率的提高，使不同部门或者

业务系统的安全策略，网络流量以及数据访问等方面具有独立性，从而避免一个地方发生安全事件而影响到全系统。

（四）入侵检测与威胁感知技术应用

在集中监控系统中，入侵检测系统（IDS/IPS）与威胁感知技术起到了实时监控、异常侦测以及安全态势感知的核心作用。入侵检测系统能够综合运用特征匹配、异常行为分析以及流量模式识别等技术,实现已知攻击与未知威胁的识别。比如通过对网络流量不正常波动、设备指令不正常或账户操作不正常等情况进行监测，能够及时地发现可能存在的攻击或者内部滥用[3]。威胁感知技术进一步融合了安全信息与事件管理（SIEM）、大数据分析以及人工智能算法，以对可能出现的威胁进行前瞻性的预测和预警，从而达到动态防护的目的。在实践中，入侵检测和威胁感知能够对攻击链进行全程监测，其中包括攻击尝试、渗透、横向移动以及目标破坏等行为。该系统可以依据风险等级引发自动化的防护策略，例如屏蔽异常流量、封禁可疑账号以及产生告警告知安全管理员。同时威胁情报平台可以通过采集外部攻击信息来预先确定对集中监控系统新的攻击方式，通过联动防御机制加以保护。定期更新优化入侵检测规则及威胁模型可以不断增强应对复杂攻击场景能力。

（五）安全日志与行为审计管理

安全日志及行为审计作为集中监控系统中安全管理的一种重要工具，在事件追溯、风险分析以及策略优化等方面起着至关重要的作用。系统要对用户的登录、操作行为、配置变更、设备事件以及网络访问情况进行综合记录，构成一个完整的可审计日志。通过对日志的集中管理以及自动化的分析工具可以实现异常行为检测、权限滥用识别以及潜在攻击的预警。比如用户经常试图进入未授权区域或者非工作时间内执行敏感操作的情况下，系统就可以触发报警，记录下详细的运行情况，从而对安全事件的调查奠定基础。行为审计既应用于事件追踪又可以引导权限优化与操作规范的建立[4]。对历史日志进行分析可以发现其中存在的管理漏洞，不恰当的操作或者不正常的使用方式，从而为制度的完善以及安全策略的调整提供数据支持。通过定期审计、合规检查与风险评估相结合的方式，能够保证系统的日常运营不断满足安全管理的要求。同时为了保证日志的完整性与可用性，要利用日志备份、加密存储以及多节点冗余等机制来避免日志被篡改或者丢失。

（六）应急响应与容灾备份机制

应急响应与容灾备份是集中监控系统应对突发安全事件和保障业务连续性的重要保障。应急响应机制应包含事件监测、告警通知、快速分析、处理方案制定及恢复操作等环节。在事件发生时，系统能够快速识别受影响的模块、评估风险范围，并按照预设流程进行隔离、阻断或修复操作，最大限度降低损失。容灾备份机制则通过数据异地备份、双活或多活部署以及业务连续性规划，确保在硬件故障、攻击破坏或自然灾害发生时，核心业务能够快速切换至备用系统，保持业务连续运行[5]。备份机制不仅包括数据，还涵盖系统配置、应用环境及操作日志等，确保恢复后系统能够快速恢复到事件前状态。结合定期演练和应急演练，验证容灾策略有效性，优化恢复时间和操作流程。同时，应急响应团队应明确职责分工、联动流程及外部支援机制，以实现从事件发现到处置和恢复的闭环管理。通过建立完善的应急响应与容灾备份体系，集中监控系统能够显著提升安全韧性，保障监控业务在各种突发情况下稳定、可靠运行。

结束语

综上所述，新一代集中监控系统网络安全防护工作是一项系统工程，必须在技术、管理、法规几个层面上采取综合措施。通过加强身份认证和访问控制机制、应用数据加密和安全传输技术、执行网络隔离和分区管理策略、部署入侵检测和威胁感知技术、强化安全日志和行为审计管理、建立应急响应和容灾备份机制等措施，能够有效增强系统网络安全防护能力。今后随着科技的进步与安全防护理念的加深，新一代集中监控系统必将更安全、更有效地为保障社会公共安全服务。

[参考文献]

[1]张丽,王守鲁. 新一代智慧变电站集中监控辅助决策系统设计与实现[J]. 电气时代，2025,（02）：80-82+86.

[2]新一代变电站集中监控系统通过实用化验收[J]. 大众用电，2023，38 （07）：37.

[3]祝宝升. 机房动力环境监控系统设计与实现[J]. 中国有线电视，2022,（01）：15-17.

[4]袁强. 网络安全事件集中监控和自动派单的设计与实现[J]. 通信与信息技术，2020,（02）：77-83.

[5]申时喜. 新一代空管设备集中监控系统发展趋势[J]. 集成电路应用，2018，35 （10）：87-88.