面向安全生产环境监控网络的安全态势感知

孙永军
焦作千业水泥有限责任公司　河南　焦作　454171

摘　要：本文针对安全生产环境监控网络面临的终端防护薄弱、数据传输风险突出、边界管控缺失等安全问题，提出基于安全态势感知技术的防护体系构建方案。首先分析了监控网络的架构特征与运行风险，论证了态势感知技术在全局监测、动态研判、主动预警方面的适配优势。其次，构建了涵盖数据采集、处理、分析、预警响应、可视化展示五层的态势感知体系，设计了核心模块功能与闭环数据流转机制。最后，针对数据采集精度不足、研判模型适配性弱、联动响应效率低等现存问题，提出分层采集适配、场景化模型构建及多维度协同处置等优化策略，为提升监控网络安全防护水平提供理论与技术支撑。

关键词：安全生产；环境监控网络；网络安全；态势感知

引言：随着工业生产自动化与智能化水平不断提升，安全生产环境监控网络已成为覆盖车间、仓储、流水线及户外点位的核心基础设施，承担着环境监测、设备管控与现场安全监控等关键职能。然而，该网络因终端分散、设备老旧、数据敏感等特征，面临终端防护薄弱、传输风险突出、边界管控缺失等多重安全威胁，传统静态被动防护模式已难以满足全天候高稳定运行需求。安全态势感知技术凭借全局监测、动态研判、主动预警等优势，为解决上述问题提供了有效路径。本文围绕安全生产环境监控网络的安全需求，系统构建态势感知体系架构，分析现存问题并提出针对性优化策略，旨在提升网络安全主动防御能力。

1 安全生产环境监控网络概述

安全生产环境监控网络是服务于工业生产现场的专用局域网系统，专为生产环境监测、设备状态管控、现场安全监控设计，覆盖生产车间、仓储区域、作业流水线、户外生产点位等全场景，是生产安全管控的核心基础设施。该网络区别于通用办公网络，核心服务于生产安全监测业务，所有运行逻辑、设备配置、数据传输规则均围绕生产监控需求搭建，具备极强的场景专用性。（1）从网络构成来看，安全生产环境监控网络主要由前端感知终端、网络传输链路、后台处理终端三部分组成。前端感知终端包含各类环境传感器、高清监控摄像头、设备工况采集模块、报警终端等，负责实时采集生产环境与设备运行的原始数据；网络传输链路依托有线光纤、工业以太网、无线专用传输通道，实现前端数据的实时上传与后台指令的下行传输；后台处理终端包括服务器、监控主机、数据存储设备，负责数据汇总、处理、存储与可视化展示，为现场安全管控提供数据支撑。（2）从运行特征来看，该网络具备三大核心特点。一是运行连续性，生产作业为全天候不间断模式，监控网络需24小时持续运行，无停机维护窗口期，对网络稳定性要求极高；二是节点分散性，监控终端分布于生产各个角落，部分终端处于复杂工况环境，设备部署零散、管理难度大；三是数据敏感性，网络传输的环境数据、设备运行数据直接关联生产安全，数据失真、丢失或被篡改会直接影响安全管控判断，对数据完整性、保密性要求严苛[1]。

2 安全生产环境监控网络安全风险及态势感知适配性

2.1 主要网络安全风险

结合安全生产环境监控网络的架构与运行特征，其运行过程中面临的安全风险主要分为设备终端风险、数据传输风险、网络运行风险三类。设备终端风险集中体现在前端监控终端防护能力薄弱，多数传感器、采集终端为专用工业设备，硬件配置简单、固件版本老旧，缺乏完善的安全防护机制，易出现终端故障、程序异常、非法接入等问题，部分终端长期运行易出现硬件老化、数据采集失效等隐性风险，难以被常规防护手段识别。（1）数据传输风险是核心安全风险之一。监控网络数据传输频次高、数据量大，且部分无线传输链路防护等级较低，易出现数据丢包、传输延迟、数据篡改等问题。同时，网络内多设备同时传输数据，易出现数据拥堵、信道占用异常等情况，导致监控数据传输不及时，造成后台监控盲区，无法实时掌握生产现场环境状态。（2）网络运行风险主要体现在网络架构防护单一、边界管控薄弱。传统监控网络架构相对封闭，长期缺乏安全迭代优化，网络边界模糊，易出现外部设备非法接入、内网异常访问等问题。同时，网络运行过程中的流量异常、

端口滥用、设备离线等隐性问题，无法被实时监测，长期积累易引发网络瘫痪、监控系统失效等重大故障。

2.2 传统安全防护模式的局限性

当前多数生产场景的监控网络防护以静态、被动防护为主，存在明显的技术局限性。（1）防护方式静态固化，依托固定的防护规则、访问权限开展防护，无法适配监控网络动态变化的运行状态，当出现新型异常行为、隐性风险时，无法实现有效识别。其次，风险识别维度单一，传统防护手段仅能针对明显的网络攻击、设备故障进行预警，无法对网络流量、设备运行状态、数据传输轨迹、终端接入行为等多维度数据进行综合分析，难以发现潜在的隐性风险。（2）传统防护模式缺乏全局研判能力，仅能针对单一设备、单一节点的异常问题进行单独处置，无法整合全网运行数据开展整体态势分析，导致管理人员无法掌握监控网络的整体安全状态，风险处置存在片面性、滞后性，难以满足安全生产监控网络全天候、高稳定、高安全的运行需求[2]。

2.3 安全态势感知的适配优势

安全态势感知技术与安全生产环境监控网络具备高度适配性，可有效弥补传统防护模式的短板。（1）具备全局监测能力，态势感知体系可覆盖全网所有终端、传输链路、后台设备，实现对网络接入、数据传输、设备运行、流量变化等全维度信息的实时采集，构建全方位的监测体系，杜绝监控盲区。（2）具备动态研判能力，可通过智能算法对实时采集的海量数据进行分析，动态更新风险识别规则，精准区分正常运行波动与异常风险，有效识别隐性、潜在安全隐患。（3）具备可视化管控能力，态势感知可将复杂的网络运行数据转化为直观的态势图像、数据报表，清晰展示网络整体安全状态、风险分布点位、风险等级，让管理人员直观掌握全网运行态势。其四，具备主动预警能力，相较于传统事后处置模式，态势感知可提前预判风险发展趋势，在风险萌芽阶段发出预警，为风险处置预留充足时间，全面提升监控网络的安全主动防御能力。

3 面向安全生产环境监控网络的安全态势感知体系构建

3.1 体系整体架构

结合安全生产环境监控网络的运行特点与安全防护需求，构建分层化、模块化的安全态势感知体系，整体分为数据采集层、数据处理层、态势分析层、预警响应层、可视化展示层五大核心层级，各层级相互衔接、协同运行，形成完整的态势感知闭环。整体架构遵循贴合生产场景、轻量化运行、精准化研判、快速化响应的原则，适配监控网络设备多、节点散、实时性高的运行特征，避免复杂架构影响网络正常监控业务运行。数据采集层为基础层级，负责全网多维度原始数据的实时采集；数据处理层对采集的异构数据进行清洗、整合、标准化处理，剔除无效数据、冗余数据，保障数据质量；态势分析层依托智能算法与研判模型，对标准化数据进行深度分析，识别安全风险、研判网络态势；预警响应层根据风险等级开展分级预警与自动处置；可视化展示层实现全网态势的直观呈现，支撑人工管控决策[3]。

3.2 核心模块功能设计

数据采集模块覆盖终端状态、网络流量、数据传输、设备行为四类数据，采集终端在线状态、硬件参数、固件运行、故障记录，全网流量大小、端口访问、协议状态，数据包完整性、传输延迟、丢包率、篡改痕迹，以及终端接入记录、权限操作、启停行为，实现全网数据无死角采集。态势分析模块采用静态规则匹配与动态智能分析结合的方式研判。通过预设安全规则，快速识别端口异常访问、终端非法接入、数据异常丢失等显性风险；通过大数据分析与机器学习算法对长期运行数据建模，精准识别流量异常波动、隐性设备故障、微量数据篡改等隐性风险，综合多维度数据研判网络整体安全态势，划分安全、预警、危险三个等级。预警响应模块依据分析结果执行分级处置：轻微异常自动记录日志并持续监测；中度风险触发声光预警与后台弹窗，提醒管理人员核查；高危风险自动阻断异常接入、隔离故障终端，防止风险扩散，保障全网稳定运行。

3.3 数据流转运行机制

安全态势感知体系采用闭环式数据流转机制，保障实时监测、实时研判、实时响应。首先由数据采集层通过分布式采集节点，全天候采集监控网络各类运行数据，实时上传至数据处理层；数据处理层对海量异构数据进行去重、纠错、格式统一，筛选有效数据并生成标准化数据集，同步传输至态势分析层。态势分析层调用预设研判模型与智能算法，对数据集进行全方位分析，生成实时网络安全态势报告，标记风险点位与风险等级；随后将态势数据与风险信息同步至预警响应层和可视化展示层，预警响应层执行对应处置策略，可视化展示层实时更新全网态势界面，最终形成“采集-处理-分析-预警-处置-复盘”的完整闭环，持续保障监控网络安全运行[4]。

4 态势感知技术应用现存问题与优化策略

4.1 现存主要问题

在安全生产环境监控网络的实际应用中，态势感知

体系仍存在多处适配性短板。（1）数据采集精准度不足，由于监控网络终端设备类型繁杂、老旧设备较多，部分老旧终端不支持高精度数据采集，存在数据采集缺失、采集延迟、数据误差等问题，导致态势分析基础数据不完整，影响研判精准度。（2）态势研判模型针对性不足，现有通用态势研判模型多适配通用网络场景，未结合生产监控网络设备长期连续运行、节点分散、数据传输高频次的专属特征，对生产场景下的正常网络波动与异常风险区分度较低，易出现误预警、漏预警问题，研判精准性不足。（3）风险响应联动性较弱，当前多数态势感知体系的预警与处置相对独立，自动处置策略较为单一，仅能应对简单的网络异常问题，针对多节点联动异常、复合型网络风险，无法实现系统化联动处置，同时人工处置与系统自动处置衔接不畅，处置效率有待提升。

4.2 针对性优化策略

针对数据采集短板，采用分层适配采集优化方案，对新型智能终端，启用全维度高精度数据采集模式，保障数据采集的完整性与实时性；对老旧不兼容终端，加装轻量化采集适配模块，优化数据采集接口与传输协议，弥补老旧设备采集短板。同时增设数据校验机制，对采集的实时数据进行实时校验，自动剔除错误数据、补全缺失数据，从源头提升基础数据质量。针对研判模型适配性不足问题，构建场景化专属研判模型，基于安全生产监控网络的长期运行数据，梳理网络正常波动规律、常见异常风险特征，优化模型算法参数，调整风险识别阈值。通过机器学习持续迭代模型，不断提升模型对生产场景专属风险的识别能力，精准区分设备正常工况波动与网络安全风险，有效降低误预警、漏预警概率，提升态势研判精准度。

4.3 体系联动效能优化

为提升风险处置联动性，优化态势感知体系的联动响应机制，搭建多维度协同处置模块。丰富系统自动处置策略，针对单一风险、复合型风险、多点异常风险等不同场景，设置差异化处置方案，实现异常阻断、设备隔离、流量调控、数据修复等多元化自动处置功能。同时打通态势感知平台与监控管理平台的数据接口，实现风险预警、设备状态、处置进度的实时同步，让管理人员可快速掌握风险全貌，精准开展人工干预。此外，增设态势复盘优化机制，定期汇总网络安全态势数据、风险处置案例，分析风险发生规律与处置短板，持续优化采集规则、研判模型与响应策略，实现态势感知体系的动态迭代升级，持续适配安全生产监控网络的运行需求，全面提升网络安全防护水平[5]。

结束语

安全生产环境监控网络作为工业生产安全管控的核心基础设施，其安全防护水平直接关系生产现场人员与设备安全。本文系统梳理了该网络的架构特征、主要安全风险及传统防护模式的局限性，论证了安全态势感知技术的高度适配性，并构建了涵盖数据采集、处理、分析、预警、可视化展示的五层态势感知体系。同时，针对当前应用中数据采集精度不足、研判模型适配性弱、联动响应效率低等问题，提出了分层采集适配、场景化模型构建、多维度协同处置等优化策略。未来需持续推动态势感知体系与生产监控业务深度融合，实现动态迭代升级，全面提升监控网络主动防御能力，为安全生产提供坚实的网络安全保障。

参考文献

[1]祝一帆,余瑞,师淑贞.面向云原生环境的微服务APl安全态势感知技术研究[J].长江信息通信,2025,38(12):148-150.

[2]曾倩倩.基于机器学习的网络信息安全态势感知系统设计[J].信息技术与信息化,2025(11):132-135.

[3]安文然.大数据网络安全态势感知中数据融合技术研究[J].现代工业工程,2025(9):109-112.

[4]陈晓宇.面向等保合规的网络安全纵深防御架构设计与验证[J].科技信息与研究,2025,5(13):43-46.

[5]孙志海.基于物联网的电厂安全监控预警系统设计[J].今日自动化,2025(4):11-13.