# 多维工控系统网络安全风险监测预警系统研究与应用*

丁朝晖，张　伟，杨国玉，刘　腾
（中国大唐集团科学技术研究总院有限公司，北京 100043）

**摘　要：** 网络安全已成为关系国家安全和发展、关系人民群众切身利益的重大问题，网络安全形势也是日益严峻，网络攻击危害政治安全、社会稳定、经济发展、文化建设，网络空间的国际竞争方兴未艾。从多个维度对潜在的网络风险进行识别和预警，在攻击成功之前采取有效措施迅速阻断攻击，是工控系统安全稳定运行的有力保障。

**关键词：** 工控系统；网络安全；监测预警
**中图分类号：** TN915.08　　**文献标志码：** A　　**DOI：** 10.16157/j.issn.0258-7998.222826

**中文引用格式：** 丁朝晖，张伟，杨国玉，等. 多维工控系统网络安全风险监测预警系统研究与应用[J]. 电子技术应用，2023，49(2)：76-79.
**英文引用格式：** Ding Zhaohui，Zhang Wei，Yang Guoyu，et al. Research and application of multi-dimensional industrial control system network security risk monitoring and early warning system[J]. Application of Electronic Technique，2023，49(2)：76-79.

# Research and application of multi-dimensional industrial control system network security risk monitoring and early warning system

Ding Zhaohui，Zhang Wei，Yang Guoyu，Liu Teng
(China Datang Group Science and Technology Research Institute Co.，Ltd.，Beijing 100043，China)

**Abstract：** Network security has become a major issue related to national security and development and the vital interests of the people. The network security situation is also becoming increasingly severe. Network attacks endanger political security, social stability, economic development and cultural construction. International competition in cyberspace is in the ascendant. This system identifies and warns potential network risks from multiple dimensions, takes effective measures to block the attack before the attack is successful, which can ensure the stable operation of the information system.

**Key words：** industrial control system；network security；monitoring and early warning

## 0 引言

当前，工业控制系统面临许多的网络安全威胁，其中，在网络安全风险识别、告警、溯源等方面面临的主要问题有：

(1) 网络安全风险警报不准确，安全运维人员忙于处理无关紧要的风险警报，而没有时间处理真正重要的告警信息。加之，安全从业人员匮乏已是众所周知，安全运维人员尤其紧缺，在这种情况下，迫切需要提高告警的准确率。

(2) 网络安全风险警报分散或不全面，虽然有的系统信息中部署了有很多网络安全检测产品，但是告警信息在不同的产品显示，由不同的人员管理，无法进行集中分析、统一处理，容易造成安全隐患处理不及时，导致严重后果。

(3) 安全工具叠加部署，安全运维人员同时管理多个设备，日常管理效率较低。

(4) 网络安全事件跟踪溯源能力较弱，需提升安全运维人员对网络安全事件的回溯能力，尤其是在工控系统故障出现以及故障查找的过程当中，日志、流量、视频数据采集到不同设备上，无法实现综合分析，无法迅速准确地确定安全事件的起因和入侵者的来源。

多维度安全风险感知系统研究是为了研究解决以上网络安全的问题，提升工控系统网络安全防护能力：

(1) 本系统研究使用AI行为建模分析，通过使用监督式学习，利用基于广义径向基函数多维度感知技术，大幅提升对已知威胁和未知威胁的识别准确率。

(2) 解决企业网络安全风险信息零散、警报分散的情况，本系统不仅支持网络全流量分析，还支持各种工

* 基金项目：2020年大唐集团第一批科技项目(KJ20-002)

控主机、安全设备、网络设备、中间件、数据库系统、软件的安全日志分析处理、视频监控图像识别，可提高工控企业网络安全风险检测能力，更全面呈现网络和物理环境中存在的安全隐患。

(3) 解决企业日常管理效率较低，本系统有助于提升工控系统的网络安全防御能力和日常管理效率，通过综合物理层面和网络层面集中监测预警信息[1]，减少安全管理的难度，提升日常管理效率。

(4) 解决企业网络安全跟踪溯源能力较差的问题，本系统可提升企业的安全事件回溯能力，尤其是在工控系统故障出现以及故障查找的过程当中，通过日志分析、流量检测、视频图像分析，高效开展全方面的调查，从而确定事故的原因和入侵的来源。

## 1 研究意义

本研究的意义是能帮助企业满足国家相关合规要求，减少网络安全投入费用，保证生产运行稳定，具体内容如下：

满足国家相关合规要求，帮助企业发现外在和内在的网络安全威胁，排查自身的风险点，全面提升工控系统的整体网络安全防护水平，优化配置策略，保证设备、网络、物理环境、应用和数据等不同层面的网络安全，满足等保2.0、信息安全风险评估、工业互联网安全评测及相关管理机构的合规要求。

减少网络安全投入费用，通过本系统可集中排查网络和物理环境中的风险隐患，有效减少企业重复部署网络安全设备的开销，节约了企业的安全运维成本。

保证生产运行稳定，根据现场设备、物联终端、控制系统、网络平台及数据安全等防护现状，确定当前资产价值、面临的威胁和内在脆弱性3个关键要素，结合业务战略、安全需求、安全事件、残余风险等属性，应用基于广义径向基函数多维度感知技术[2]进行安全诊断，实现工控系统安全风险识别和预警，并保证工控系统的安全生产稳定运行。

## 2 系统原理

多维度安全风险感知分析系统研究主要基于大数据技术[3]、人工智能技术[4]，发现安全事件进行准确的挖掘，通过全方面的战略部署，将工业企业的运行、检修、安全团队整合，实现网络安全、物理安全的主动防御和全方面的数据分析[5]。

基于广义径向基函数的神经网络安全态势模型由输入 $\boldsymbol{X}=\{x_1,x_2,\cdots,x_n\}^{\mathrm{T}}\in\boldsymbol{R}^n$、网络权值 $\boldsymbol{W}=\{w_1,w_2,\cdots,w_m\}^{\mathrm{T}}\in\boldsymbol{R}^{L\times m}$、阈值 $\boldsymbol{V}$、求和单元 $\sum(\,)$、激励函数 $f(x)$、神经网络输出 $\boldsymbol{Y}=\sum_{i=1}^{L}w_{ij}\varphi_j,j=1,2,\cdots,m$ 组成。

将流量、日志、视频数据经过分析处理后形成训练样本 $\boldsymbol{X}=\{x_1,x_2,\cdots,x_n\}^{\mathrm{T}}\in\boldsymbol{R}^n$，隐含层第 $j$ 个神经元节点的输出计算公式为：

$$\varphi_j=\mathrm{e}^{-\frac{\|x-c_j\|^2}{2\sigma_j^2}},j=1,2,\cdots,m \tag{1}$$

其中，$c_j$ 为隐藏层第 $j$ 个节点的高斯函数中心点。隐含层的所有输出为：$\boldsymbol{\Phi}=\{\varphi_1,\varphi_2,\cdots,\varphi_L\}^{\mathrm{T}}\in\boldsymbol{R}^L$，神经网络的输出是对隐藏层输出加权计算的结果：

$$\boldsymbol{Y}=\sum_{i=1}^{L}w_{ij}\mathrm{e}^{-\frac{\|x-c_j\|^2}{2\sigma_j^2}},j=1,2,\cdots,m[6] \tag{2}$$

在训练时，学习率取0.03。训练过程如下：

(1) 各层的权值 $\boldsymbol{W}$ 随机输入；

(2) 根据训练目标进行对各层的权值调整，训练以预测值与标签的均方误差MSE≤0.01时达到训练要求；

(3) 训练结束，模型参数随之确定。

通过实验对比，基于广义径向基函数的多维度安全风险感知模型的预测结果与安全实际态势基本相同，模型预测准确率和召回率极高，优于基于时间序列的预测模型[7]和基于回归分析的预测模型[8]。

## 3 系统框架

本系统采用大数据存储处理+流量采集探针+视频监控设备的理念进行构建，基于分布式架构的高性能大数据智能安全分析平台，设计由单台高性能服务器（内置虚拟化集群）或多台服务器集群组成，使用基于广义径向基函数的多维度安全风险感知模型，并结合数据挖掘、人工智能等技术；具备海量数据采集存储、高性能分布式计算、实时分析与告警、可视化展示及安全报表等功能；实现模块间低耦合、模块内高内聚，主要分为基础平台层、微服务架构层和数据展示层，如图1所示。


图1 系统框架图

(1) 基础平台主要包括设备层、数据采集层、数据存储层，采用分布式大数据架构，实现全流量数据高性能收集、分发和存储，给安全风险的感知分析提供海量数据基础[9]。

(2) 微服务架构层将平台安全分析功能模块化，作为多个安全服务嵌入到平台之中。包括资产发现模块、资产拓扑算法模块、AI聚类算法模块、AI检测模块、关联分析模块、风险回溯模块、视频分析模块，可灵活进行扩展和升级。

(3) 数据展示层针对安全检测和分析的结果进行可视化呈现，主要包括风险感知显示、多维风险告警、安全报表、资产管理、安全事件分析等。通过可视化呈现，让安全风险无处遁形，可见可控。

## 4 主要研究内容

多维度安全风险感知分析系统的目标是实现基于分布式架构的高性能大数据智能安全分析平台，搭载了独创的AI威胁免疫算法防止恶意程序运行，并结合了机器学习、数据挖掘、神经网络等技术，弥补工业控制企业网络安全和物理安全方面的不足，主要研究内容如下：

(1)研究广义全流量分析[10]，方便运维人员进行统一风险分析和管控，不依赖先验的攻击特征或威胁情报，无需特征库或威胁情报库升级，无需连接云端，通过不断学习现网中的流量进行自我迭代和自我强化，持续地学习每一个子网，每一台资产的日常流量模型。同时，通过与同类设备横向对比，以及与资产自身历史行为的纵向对比，持续地检测不同资产的异常行为，找到不符合日常规律的隐秘异常行为，发现未知威胁。

(2)研究安全日志[11]流量视频数据的多维度风险预测，研究将日志数据和流量信息、视频数据集中收集和分析，集日志审计和全流量深度解析[12]、视频监控违规识别功能于一体，实现安全风险全方位感知和安全事件跟踪溯源、检测预警、统筹管理等功能。其中，安全事件跟踪溯源展示如图2所示。


图2 安全事件跟踪溯源展示

(3)研究智能视频监控违规行为告警及事件跟踪技术[13]，采用深度学习算法[14]研究提升对视频监控信息的处理和优化能力，通过对视频数据的智能分析，实现黑名单告警、陌生人告警、轨迹查询、出入人数统计、人流量统计、安全帽佩戴检测、工作服检测、物品遗留侦测、使用手机侦测、烟火报警、火点识别、柜门开关检测等功能，并能进行违规行为分析告警、违规事件跟踪，按告警信息类别展示告警信息等，智能视频监控违规行为展示如图3所示。

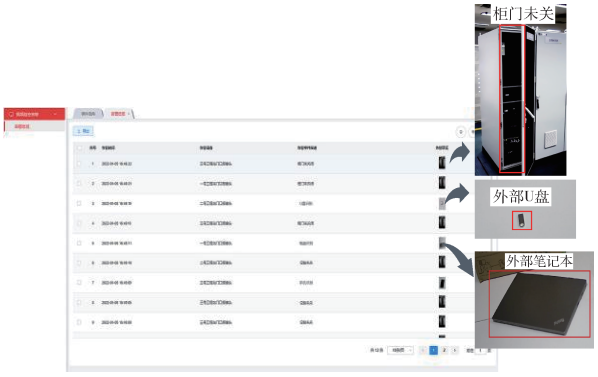


图3 智能视频监控违规行为展示

(4)研究高效资产运维及拓扑可视化技术[15]，针对大中型工业企业资产数量多、维护难的特点，多维度安全风险感知分析系统通过流量信息发现环境中各个资产，无需手动录入；发现后可灵活进行资产分组和资产标识，极大方便未知资产识别及资产管理。通过人工智能算法，自动进行资产聚类，识别资产流量拓扑，展示单个资产访问关系拓扑，识别异常访问。

## 5 应用情况

本系统应用后产生的社会效果如下：

(1)重保、冬奥会时期，为电力企业稳定运行保驾护航成绩显著，流量日志视频数据聚合及精准威胁告警、风险监测和网络安全事件追溯，多维度网络安全风险感知分析系统采用AI模型进行威胁检测，区别于传统安全感知设备，克服了传统设备告警数量巨大、误报率高的缺点，在重保、冬奥会时期，发出了数千条告警信息，工作人员及时处理，减少应用单位由于网络安全攻击造成的声誉和经济损失。

(2)提升网络安全应急响应和溯源能力，解决工控企业网络安全跟踪溯源能力较差的问题，提升应用单位的安全事件溯源能力，尤其是在故障出现时，通过日志分析、流量检测、视频图像分析，高效开展全方面的调查，能够迅速确定事故的原因和入侵的来源，从根源上消除安全隐患。

(3)降低了网络安全风险误报率，提高网络安全事件处置效率，解决工控企业日常管理效率较低，本系统有助于提升工控系统的网络安全防御能力和日常管理效率，通过综合物理层面和网络层面集中监测预警，减少安全管理的难度，保证管理员对于安全风险第一时间进行处置和响应。

(4)有效防控“勒索病毒”，本系统利用流量日志视频数据聚合分析，发现流量或日志中勒索病毒活动迹象

后，迅速进行告警，提示安全工作人员进行处理，并能在发现“勒索病毒”入侵后，通过对流量日志视频数据分析调查，找到“勒索病毒”入侵来源和跳板，清除病毒毒窝，切断攻击者入口。

(5)降低网络安全投入费用，本系统可减少分别采购日志收集与分析系统、流量分析系统、视频告警平台的投入，减少重复投资，为企业节省信息安全方面的开支，每年度可节约安全投入费用几十万元。

## 6 结论

本文研究的多维工控系统网络安全风险监测预警系统集日志审计和全流量深度解析、视频监控违规行为于一体，极具实用价值，意义巨大，实现了网络安全风险全方位感知、安全事件跟踪溯源、监测预警、统筹管理等功能，全面提升发电企业的整体网络安全防护水平，经济效益和社会效益非常显著，具有极高的推广应用价值。

目前，本系统主要实现网络安全监测预警功能，在下一步的工作中应注重主动防御功能的实现，条件允许的情况下实现及时阻断网络攻击，保障工控系统安全稳定运行。

**参考文献**

[1] 邱丹骅.电网调度监控系统的节点安全度感知与预警技术分析[J].电子技术,2021,50(11):294-296.
[2] 王刚.SoS体系多维度分析在信息安全风险评估中的应用[J].微型电脑应用,2020,36(9):56-59.
[3] 石光捷,张良,付飞龙,等.基于行为特征大数据分析的网络行为风险感知及防御方法[P].CN110798353A,2020-02-14.
[4] 杜涛.基于BP神经网络技术的网络流量预测模型[J].网络安全技术与应用,2016(7):55,57.
[5] 李天骐.基于神经网络的网络安全态势评估与预测技术研究[D].北京:华北电力大学,2016.
[6] 薛丽敏,李忠,蓝湾湾.基于在线学习RBFNN的网络安全态势预测技术研究[J].信息网络安全,2016(4):23-30.
[7] 张威.网络安全告警的时间序列分析及预测[D].武汉:华中科技大学,2008.
[8] 王宇飞,沈红岩.基于改进广义回归神经网络的网络安全态势预测[J].华北电力大学学报,2011,38(3):91-95.
[9] 阮晓龙,冯顺磊.基于ELK的Windows系统安全风险分析的研究探索[J].软件,2019,40(11):202-207.
[10] 刘立,陈明宇,包云岗,等.一种基于页面级流缓存结构的流检测和预取算法[J].计算机研究与发展,2009,46(10):1758-1767.
[11] 吕智慧,刘思帆,吴杰.一种基于主机日志分析的云数据中心实时风险评估方法[P].CN104125217A,2014-10-29.
[12] 杨姗媛.信息安全风险分析方法与风险感知实证研究[D].北京:中央财经大学,2015.
[13] SONG Y, LUO W, LI J, et al.SDN-based Industrial Internet Security Gateway[C]//2021 International Conference on Security, Pattern Analysis, and Cybernetics (SPAC), Chengdu, China, 2021:238-243.
[14] SAFDAR A, DURAD H, ALAM M. Design and implementation of real-time visualization tool for network security monitoring[C]//2018 15th International Bhurban Conference on Applied Sciences and Technology (IBCAST), Islamabad, Pakistan, 2018:477-483.
[15] PRARTHANA T S, GANGADHAR N D.User behaviour anomaly detection in multidimensional data[C]//2017 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM), Bangalore, India, 2017:3-10.

（收稿日期：2022-04-07）

**作者简介：**

丁朝晖(1977-)，女，硕士研究生，高级工程师，主要研究方向：网络安全、工控系统安全。

张伟(1976-)，男，硕士研究生，高级工程师，主要研究方向：网络安全、工控系统安全。

杨国玉(1980-)，男，硕士研究生，高级经济师，主要研究方向：信息化与网络安全管理。

扫码下载电子文档

# 版权声明