 DOI: https://doi.org/10.12349/iser.v6i9.7456

Research on Industrial Control Network Security Situation Awareness Model and Visualization Technology

Yao Ma

Ningdong Aluminum Branch of Qingtongxia Aluminum Industry Co., Ltd., Yinchuan, Ningxia, 750100, China

Abstract

Industrial control networks are the core support for production automation and intelligent management, and play an important role in the transformation and upgrading of the manufacturing industry in the new era. The article takes situation awareness and visualization as the key points to ensure the security of industrial control networks. It constructs an industrial control network security situation awareness model from three aspects: data collection, data processing and analysis, and early warning and response. It discusses the commonly used visualization tools, analyzes the challenges in industrial control network security situation awareness and visualization, and proposes countermeasures.

Keywords

Industrial control network; Security posture; Perception model; Visualization technology

工控网络安全态势感知模型及可视化技术研究

马瑶

青铜峡铝业股份有限公司宁东铝业分公司，中国 · 宁夏 银川 750100

摘　要

工控网络是生产自动化、管理智能化的核心凭借，在新时期制造业转型升级中占据着重要的地位。文章将态势感知与可视化作为保障工控网络安全的要点，从数据采集、数据处理与分析、预警与响应三个层面，构建了工控网络安全态势感知模型，探讨了常用的可视化工具，并分析了工控网络安全态势感知与可视化中的挑战，提出了应对策略。

关键词

工控网络；安全态势；感知模型；可视化技术

1 引言

工业控制网络（工控网络）是专为工业自动化系统设计的通信网络基础设施，具有实时监控、精确控制生产过程的功能，在提高生产效率，保障生产安全中发挥着重要的作用。近年来，随着工业与互联网的深度融合，工控网络逐渐从封闭架构转向开放互联 [1]。这使得工控网络面临的安全风险更为多样、复杂。态势感知与可视化是工控网络安全风险防控的两大要点，前者在数据采集的基础上，依托态势感知模型，动态监测、分析网络威胁，后者采用可视化技术，将态势感知结果，以图表等直观、形象的工具呈现出来。态势感知与可视化的联合运用，能显著提升工控环境的安全防御能力与应急响应效率。

【作者简介】马瑶（1996–），女，回族，中国宁夏银川人，本科，助理工程师，从事电解铝行业信息化、网络安全方向研究。

2 工控网络安全态势感知模型

2.1 数据采集层

数据采集是工控网络安全态势感知的基础，数据采集是否全面、完整，对态势感知的结果有着直接的影响。应构建覆盖工控网络区域边界、网络通信节点以及计算环境的数据采集机制，消除数据采集中的漏洞、死角。首先，部署网络探针。工控网络为复杂的网络系统，包含多种类型的设备，如 PLC、传感器、SCADA 服务器等。这些设备的通信协议并不一致，常见的有 Modbus 协议、Profinet 协议、DNP3 协议等。差异化的通信协议，对数据采集的兼容性提出了更高的要求。可采用旁路监测模式，部署网络探针，实时捕获数据的同时，避免对正常生产通信造成干扰。其次，部署协议适配模块。针对异构设备的数据兼容问题，可在数据采集层部署协议适配模块，通过专用解析插件的开发与应用，将来源不同、类型多样的数据，转化为标准的结构化数据，为数据的集中处理提供条件。最后，引入数据校验机制。采集而来的数据中，存在着大量的噪声数据，如设备临时故障产生的异常日志。可引入数据校验机制，将噪声数据过滤出去，

保障数据的真实性、可靠性。

2.2 数据处理与分析层

数据处理与分析是工控网络安全态势感知模型的核心，主要利用大数据、人工智能，充分挖掘数据价值，实现工控网络安全态势的精准评估与动态预测。

首先，数据清洗与特征提取。数据清洗方面，数据校验机制的引入，虽然能过滤部分噪声数据，但采集而来的数据中，仍存在大量的冗余信息、异常值。可通过结构化缺失值填补、重复值处理、异常值检测，清洗异常数据，确保数据质量 [2]。特征提取方面，从结构化数据中，提取能有效反映工控网络运行状态、潜在威胁的特征指标。例如，从设备日志中提取操作账号、指令类型、参数修改记录等特征指标，从流量数据中提取会话时长、数据包大小分布、协议交互频率等特征指标。

其次，模型分析。结合工控网络的行为特性选择适配的算法。工控网络正常运行时，设备的通信模式、操作流程相对固定，可采用无监督学习算法进行异常检测，如孤立森林算法能快速识别与正常行为差异较大的异常数据，自编码器则可通过重构正常数据的特征，对偏离重构范围的异常行为进行定位。针对已知威胁，可采用基于特征匹配的检测算法，将提取的特征与威胁情报库中的攻击特征，如恶意软件的签名、攻击 IP 的行为模式等进行比对，实现精准识别。

最后，量化评估。围绕设备运行状态、威胁严重程度、漏洞存在情况等，设计评估指标，并赋权，形成工控网络安全评估指标体系，将工控网络安全态势转化为直观的安全指数，指数越低表明安全风险越高，便于管理人员快速掌握整体安全状态。

2.3 预警与响应层

预警与响应层为工控网络态势安全感知模型的输出环节，能够根据数据处理与分析的结果，生成警告，并依托动态反馈机制，持续优化响应策略，从而保障工控网络安全。首先，构建分级预警机制。工控网络运行中的安全风险较为多样，不同安全风险的发生几率、紧急程度以及危害性有着很大的差异性。应在风险识别、评估的基础上，将风险划分为一般、较大、重大三个等级，并构建分级预警机制。对非授权 IP 的端口探测等一般风险，可通过日志记录与定期统计分析进行处置。对针对 SCADA 服务器的漏洞利用尝试等较大风险，应立即通知运维人员，开展漏洞修复，以防风险扩大。对恶意篡改 PLC 参数等重大风险，自动触发切断攻击源与目标设备的网络连接、启动备用设备切换流程等应急响应措施，以防攻击对生产安全造成影响。其次，优化动态反馈机制。预警准确性对于工控网络安全风险防控尤为重要，而动态反馈机制，则是提升预警准确性的关键。举例而言，系统会录每一次预警的处置结果，若某类预警多次被判定为误报，则自动优化分析模型，降低误报几率。

3 工控网络安全态势感知结果可视化技术

3.1 多维展现形式

可视化的核心，是借助图像、图形、表格等直观、具象的工具，多维呈现态势感知的结果，满足不同场景下安全监控的需求。常用的可视化工具主要有拓扑图、热力图、雷达图等。可根据工控网络安全风险防控的实际需要，选择针对性的可视化工具，并协同发挥好各类工具在保障工控网络安全中的作用。

表 1 常用可视化工具表

图表类型	特点	适用范围	作用
拓扑图	1. 采用分层绘制方式，覆盖物理层、网络层、应用层，分别呈现设备部署位置、设备间连接关系、运行的工控系统与服务。 2. 通过颜色编码区分设备状态，绿色代表正常运行，黄色代表存在异常，红色代表发生故障或被攻击	工控网络整体结构展示，需全面呈现设备部署、通信链路及系统服务分布的场景，如工厂工控网络、能源行业 SCADA 系统网络等。	帮助管理人员快速定位异常设备的具体位置，同时明确异常设备的关联节点，为故障排查与攻击溯源提供直观指引。
热力图	1.以地理区域或设备类型为单位划分展示范围。 2. 通过颜色深浅直观反映威胁发生的频率与严重程度，颜色越深表示威胁越集中或级别越高	大型工控场景中威胁分布情况展示，如大型工厂、跨区域能源管网等。	清晰呈现高威胁区域，提示管理人员重点排查颜色较深的区域，判断是否存在持续攻击行为，提升威胁排查的针对性。
雷达图	1. 以资产风险、威胁风险、漏洞风险、运维风险为多维度坐标轴。 2. 坐标轴刻度代表对应维度的风险得分，通过图表形状可直观识别各维度风险差异	工控网络多维度风险综合评估场景，需同时分析资产、威胁、漏洞、运维等不同层面风险状况的情况。	帮助管理人员快速判断当前网络的主要风险短板，明确风险源头，进而指导优先开展的安全工作。

3.2 实时更新与交互

实时更新与交互，是动态反馈工控网络安全态势的关键。D3.js 框架支持复杂图形绘制与交互，在工控网络安全态势感知可视化中，具有良好的适配性。基于 D3.js 框架，开发可视化界面，从实时更新的角度而言，可将可视化系统与后端流处理框架联动，Spark Streaming 等后端流处理框架，将数据处理与分析的结果，实时推送至前端，前端则通过异步刷新技术，动态更新可视化界面，便于安全人员把握工控网络安全情况。举例而言，当系统检测到针对工控网络的供给行为时，流处理框架依据不同来源的数据，从攻击目标、

攻击类型、影响范围等方面开展分析，将分析结果推送至前端，拓扑图、热力图、雷达图等可视化工具，及时更新。从交互的角度而言，可视化界面提供钻取分析、筛选查询等操作。安全人员可根据实际需要，与可视化界面交互。举例而言，当界面将某台设备的颜色标准为红色时，安全人员点击界面，便能获取设备型号、IP 地址、近期运行日志、关联流量数据、历史安全事件等更为详细的信息，从而精准把握设备运行状态。

4 工控网络安全态势感知与可视化的挑战与对策

4.1 挑战分析

态势感知模型与可视化技术能有效提升工控网络安全风险防控能力，然而，实践层面，态势感知模型与可视化技术的应用，仍面临着多重挑战。

一是实时性不足。工控网络对响应速度要求极高，部分攻击行为如参数篡改、指令注入可在秒级内对生产造成影响。现有分析模型中复杂的机器学习算法，如深度学习模型推理耗时较长，流处理框架在处理高并发数据时也可能出现延迟，导致告警与响应滞后，错过最佳处置时机。

二是准确性有待提升。工控网络中设备类型多样、协议复杂，设备启停、工艺调整等正常生产行为产生的数据与异常威胁数据相似，易被模型误判为攻击。同时，针对 5G 工业网关的未知攻击等新型工控威胁缺乏特征库支持，导致模型漏报，影响态势评估的精准性。

三是互操作性差。不同厂商的工控设备、安全产品采用差异化的协议与数据格式，如甲厂商的态势感知系统与乙厂商的防火墙无法直接互通数据，告警信息与日志格式不统一，导致多系统协同监测时出现数据孤岛，无法形成完整的态势视图。此外，部分老旧工控设备，如运行超过 10 年的 PLC，缺乏标准化的接口，难以接入态势感知系统，易形成监测盲区。

4.2 应对策略

实时性、准确性、交互性等方面的挑战，严重影响了态势感知模型与可视化技术在保障工控网络安全中的作用。对此，应采取有效的策略，全面改进态势感知模型与可视化技术，切实提升工控网络安全水平。

针对实时性不足的问题，可从模型优化与边缘计算部署两方面入手。模型优化方面，采用轻量化算法替代复杂算法，如将深度学习模型通过 TensorRT 工具进行量化压缩，减少模型参数与计算量，降低推理延迟。对算法流程进行简化，如在边缘节点先采用简单的规则匹配筛选出疑似异常数据，再将疑似数据传输至中心节点进行深度分析，减少数据传输量与中心节点的处理压力 [3]。边缘计算部署方面，在工厂车间、区域变电站等靠近数据采集点的位置部署边缘计算节点，实现数据的本地化处理，如边缘节点可实时分析 PLC 设备的运行数据，发现异常时本地触发简单响应，无需等待中心节点的指令，大幅缩短响应时间。

针对准确性有待提升的问题，可构建多模型融合体系，并打造威胁情报库。不同算法，在数据分析、风险识别、危害研判中，有着不同的优势和适用范围。举例而言，孤立森林算法具有快速异常检测能力，能够在最短的时间内找出异常，基于威胁情报的特征匹配算法则具有精准识别能力，能够精准定位风险。可构建多模型融合体系，协同发挥各类算法在风险识别中的作用，有效解决单一算法导致的偏差问题。威胁情报库的构建，能够提升态势感知模型对新型威胁的识别能力。应以企业内部的历史安全事件数据为基础，全面整合行业专用威胁情报，打造本地化的情报库，同时，做好情报库的动态更新。

针对交互性差的问题，应从老旧设备改造以及标准化建设两个方面采取好措施。老旧设备改造方面，对已经无法接入系统的老旧设备，可部署外挂式采集模块，以非侵入式方式获取设备数据。以老旧 PLC 为例，可在通信线路旁部署信号采集器，解析设备的通信数据。同时，结合新形势下工控网络安全风险防控的需要，制定老旧设备的替换计划，以具备标准化接口、安全功能的新型设备，逐步替换老旧设备。标准化建设方面，不同厂商系统数据共享性差，使得工控网络安全态势感知中存在着数据孤岛的问题。可采用 OPC UA for Security 等工控安全标准统一数据交换格式，并围绕互联互通规范、接口协议、数据结构以及预警格式等方面，推进行业标准化建设。

5 结语

工控网络安全态势感知模型的构建以及可视化技术的应用，能够有效提升工控网络安全风险防控能力。应深刻认识到态势感知、可视化的作用，并结合当前面临的问题，从实时性、准确性、交互性三个方面，采取好策略。

参考文献

[1] 王海达，杨龙保，胡传超.流域集控中心工控网络节点安全态势感知方法探析[J].数字技术与应用，2025（02）：77-79.

[2] 王强.基于GWO-GRU的工控网络安全态势预测模型分析[J].计算机应用文摘，2023（17）：123-125.

[3] 张晋宾.工控网络安全新兴理念及发展态势分析[J].自动化博览，2024（01）：16-21.