基于零信任架构的工业终端安全防护技术研究

孙国锋[1]，曾　彬[2]，唐　宁[1]

（1. 中核二七二铀业有限责任公司，湖南　衡阳　421004；2. 长沙学院，湖南　长沙　410000）

摘　要：工业系统涉及的设备、产品门类繁杂，工业信息系统安全边界逐渐模糊，外部攻击和内部威胁日益严重。聚焦解决工业互联网边缘管理存在的安全隐患，研究适应于不同种类终端、不同接入和交互方式的统一身份认证、持续信任评估、动态访问控制技术，构建了面向工业信息安全的零信任安全防护架构，能够规避非法仿冒接入、安全漏洞利用、数据监听窃取等安全风险，监测接入工业设备的通信行为特征，实现接入可信、协议安全、持续评估的防护目标，从而提高工控网络边界主动防御能力。

关键词：零信任；工控网络；访问控制；安全防护

中图分类号：TP309　　**文献标识码：**A　　**DOI：**10. 19358/j. issn. 2097 - 1788. 2025. 09. 004

引用格式：孙国锋，曾彬，唐宁. 基于零信任架构的工业终端安全防护技术研究［J］. 网络安全与数据治理，2025，44(9)：22 - 28.

Research on key technologies of industrial terminal security protection based on zero trust

Sun Guofeng[1], Zeng Bin[2], Tang Ning[1]

(1. CNNC 272 Uranium Industry Co., Ltd., Hengyang 421004, China; 2. Changsha University, Changsha 410000, China)

Abstract: The industrial system involves a wide variety of equipment and products, and the security boundary of industrial information systems is gradually blurring. External attacks and internal threats are becoming increasingly serious. This paper focuses on solving the security risks existing in the edge management of the industrial Internet, studies the unified identity authentication, continuous trust assessment, and dynamic access control technologies that are suitable for different types of terminals, different access and interaction methods, and builds a zero-trust security protection architecture for industrial information security. It can avoid security risks such as illegal imitation access, security vulnerability exploitation, and data monitoring and theft, monitor the communication behavior characteristics of industrial devices connected to the network, and achieve the protection goals of trusted access, protocol security, and continuous assessment, thereby improving the active defense capability of the industrial control network boundary.

Key words: zero trust; industrial control network; access control; security protection

0　引言

目前，工业控制系统（Industrial Control System，ICS）的建设规模不断扩大，复杂程度不断提高，导致其面临的安全风险激增，例如误操作、数据篡改、未授权访问，以及恶意代码、拒绝服务、违规外联、异常进程活动等外部威胁[1]。基于对系统内设备、应用和用户的信任，传统工控网络安全架构在一定程度上已不能完全满足目前工业信息系统日益复杂的安全防护要求。零信任机制适用于工业互联网中设备多样性和网络边界模糊的特点，通过身份验证、持续信任评估与动态调整访问控制等策略，为工业互联网安全提供了重要解决方案[2]。为了解决传统安全防护体系在新型工业终端接入管控方面逐渐失效的问题，本文紧密围绕新型工业终端接入安全管控需求，深入研究以工业主机、控制设备、非受控终端等为代表的终端统一身份认证、持续信任评估、动态访问控制等技术，进而研制面向新型业务终端接入的威胁智能防控系统原型，实现工控网内终端设备的有效识别、行为监测与异常管控，提高工业互联网的边界智

能安全管控能力，构建面向异构工业终端的多层次边界接入防护体系。

1 研究背景

随着业务云的发展，基于安全过滤策略的传统工业防火墙对于网络边界模糊的场景越来越无能为力，工业网络面临的安全攻击风险也越来越大[3-4]，具体挑战及需求包括：

（1）智能身份分析。目前工业设备、终端的接入管理不够精细，对终端资产、软件配置、异常操作及违规行为缺乏有效的监测与管控手段，且缺失终端准入标准化流程。因此，亟需基于智能身份治理分析来重建信任，实现智能化的终端设备发现与管控[5-6]。

（2）业务安全访问。业务隐藏于可信接入网关之后，只对合法用户/设备可见，可信接入网关既充当策略执行点，又承载流量加密能力，使得终端使用人员行为无法管控[7]。

（3）动态访问控制。当前远程接入认证为一次性静态认证方式，缺乏动态持续认证措施，一旦出现风险将无法应对。特别是高敏感业务访问面临巨大威胁，终端自身安全性无法保障[8]。

通过对典型工业环境现有接入终端进行全面梳理及威胁分析，当前迫切需要研究满足工业场景下终端网络安全防护特殊性和最小化改造需求。而零信任（Zero Trust，ZT）模型打破了旧式边界防护思维，依靠身份认证与访问管理、编排、分析、加密、系统权限等技术来完成安全防护，可以实现对工业互联网新型业务终端的无改造非侵入式统一身份认证、持续的交互行为安全评估以及适应安全需求的动态访问控制[9-10]。

2020 年，美国国家标准与技术研究院发布了零信任架构（Zero Trust Architecture，ZTA）的通用部署模型及推广标准[11]。近两年，国内外网络安全产品厂家正在开展大量零信任网络安全防护相关研究[12]，相关产品可以适应于不同种类终端、不同接入和交互方式的统一身份认证、持续信任评估、动态访问控制技术，着力解决非法终端接入、合法终端被盗用、合法终端恶意非授权访问和破坏等问题[13]。

从 2022 年开始，零信任在工业领域得到广泛关注，使用范围不断扩展，从为关键工业设备及 ICS 提供防护边界到全面的工业控制网络安全保障，零信任对工业场景的适配程度不断提升[14]。但总体而言，零信任在工业互联网中的研究与应用仍处于起步阶段，亟需更加全面且系统的探索[15]。

2 基于贝叶斯网络的终端可信度评估

零信任架构在工业网络中能否成功应用的关键在于其是否可以根据终端的动态行为特征去准确判断终端的风险程度与可信度。而终端的行为因素是动态变化的，比如流量变化率、攻击次数、异常连接、中高危端口等，为了准确评估终端的可信度，本文采用贝叶斯网络有效提升评估的精确性与适应性，将终端可信度评估任务转化为一系列条件依赖关系的计算。

贝叶斯网络是描述数据变量之间依赖关系的图形模型[16]。设 $G=(V, E)$ 表示一个无环有向图，其中 V 是图形中所有节点的集合，E 是所有有向边的集合，随机变量节点 $X_i \in V$ 代表一个评估因素（如流量变化、异常连接等），则这些变量的联合概率分布可以表示为下式：

$$P(X_1, X_2, \cdots, X_n) = P(X_1)P(X_2 \mid X_1), \cdots, P(X_n \mid X_1, X_2, \cdots, X_{n-1}) \tag{1}$$

通过定义节点间的条件概率，可以推算出终端的最终可信度，简化如下：

$$P(X_1, X_2, \cdots, X_n) = \prod_{i=1}^{n} P(X_i \mid \text{Parents}(X_i)) \tag{2}$$

其中，Parents 表示 X_i 的前驱节点，联合概率值可以从相应条件概率表中查到。本文的风险评估模型包含四个重要变量：流量变化率 S、攻击次数 A、异常连接数 L 和中高危端口数 H。其中 S、L 通过深度数据包检测结合采样算法可以间接推断，A 和 H 通过安全扫描检测可以直接观察。

以流量变化率 S 为例，通过数据包深度检测技术进行采样，$Y=\{y_i, i=1, 2, \cdots, n\}$ 为样本值对应采集数据包的集合，$X=\{x_i, i=1, 2, \cdots, n\}$ 为样本点位置信息集合，$s_i=(x_i, y_i)$ 表示 S 中的第 i 个元素，则在该段时间区域内网络流量变化率计算如下式：

$$S(X, Y) = \frac{\sum_{i=1}^{n} \left| f_i^K(x_i) - y_i \right|}{(x_n - x_1)}, 1 \leqslant i \leqslant n \tag{3}$$

其中，$f_i^K(x_i)$ 是对 S 的线性回归，流量变化率能准确捕捉到终端的异常流量突发带来的风险。因此，终端风险评估就划归为通过 S、H、L、A 的观察值进行概率推理。

3 系统设计

本文重点研究新型工业终端安全接入和威胁智能防控关键技术。实现方案无需对现有网络进行修改，具有动态自适应、开放可编程和持续评估的特点。且无需终端安装代理或软件开发工具包（SDK），避免了终端接口改造问题。考虑对现有网络改造最小化的要求，基于零信任的安全可控系统平台部署在云平台侧，实现子模块

的统一 API 访问代理、统一身份认证、数据采集分析、终端指纹构建、终端信任度持续评估，以及终端跨区域、跨层级、跨系统的动态访问控制等功能。结合深度数据包检测（Deep Packet Inspection，DPI）等流量采集与挖掘分析技术，多数据源融合联动分析，AI 智能建模分析，持续性监听已知工控网络中的未发现资产，实现全面的终端设备资产、流量、性能与安全管理。设计方案架构如图 1 所示。

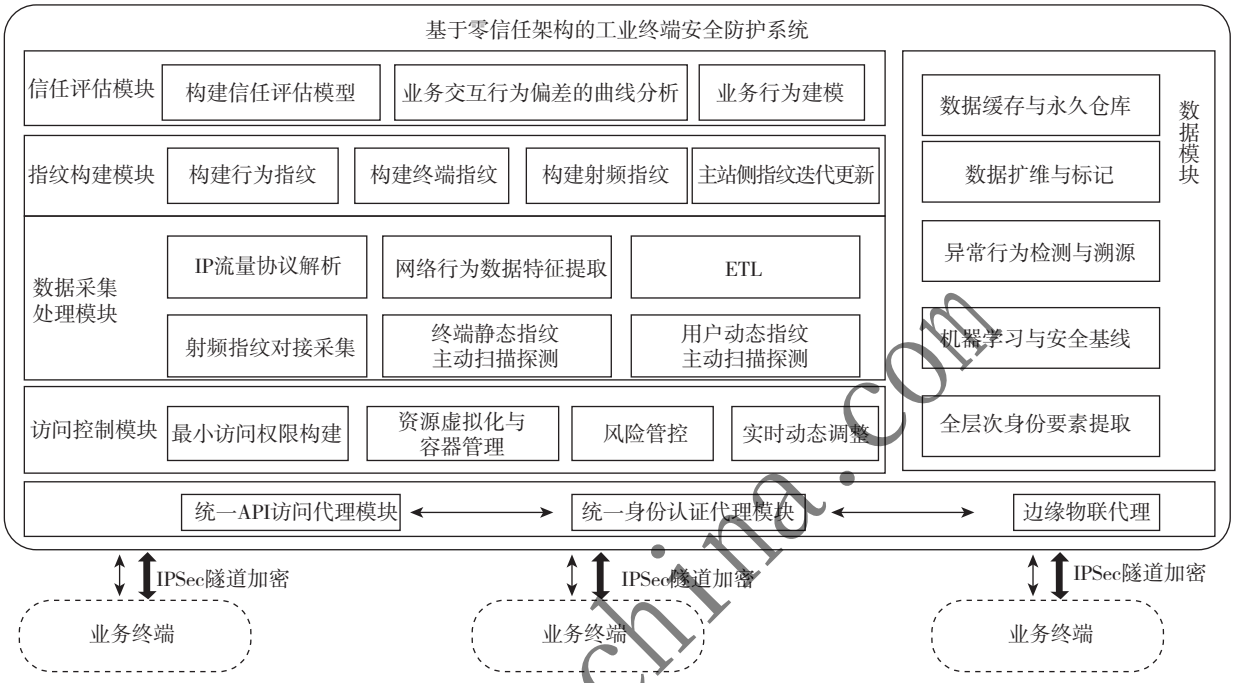

图1　系统设计架构图

身份认证模块：建立网内终端的特征指纹库，对所有受控和非受控终端的访问请求，实施集中的匹配验证。通过可信验证的终端才能访问网内业务系统。通过集中代理 API 调用者发送的访问请求，验证访问请求中代表调用者的身份和权限的凭证，实现对未知身份的访问请求的拦截，对正常访问请求进行转发。

访问控制模块：基于零信任理念，根据终端的当前属性（环境、身份、行为、信任度），生成实时访问控制规则，保证内网资源最小权限访问。支持终端访问策略的动态调整，特别是对可疑终端的行为实时监测与风险评估，及时触发缩权访问或阻断机制。

数据采集/指纹构建模块：该模块用于对用户身份的识别，采用主被动探测方式构造特定数据探测帧。通过构造特定数据探测帧，对终端主动探测，对响应数据进行分析，提取出终端设备硬件特征、协议特征、网络流量行为特征和业务协议访问特征，最终实现“终端－软件－用户”全层次身份要素提取，提取出抗伪造的工业终端指纹，构建统一的接入终端行为指纹，实现非受控身份识别。

信任度评估模块：系统支持多种数据采集技术，包括网络探针、简单网络管理协议（SNMP）、第三方接口、端口识别等，可使用协议数据包行为特征分析及数据挖掘技术对设备行为画像。对业务交互行为进行学习分析，构建非受控终端的业务安全基线。然后以终端业务安全基线为基础，根据业务交互行为，进行持续的区分不同参数的非受控终端信任度评估。

4　关键技术

4.1　面向指纹构建的资产扫描、识别技术

工控网络终端的资产特征指纹采集与发现是构建基于零信任的终端安全防护的前提与基础。本文实现的途径是主动发包探测与被动流量分析相结合方式，如图 2 所示。首先构造主动探测包，扫描搜集终端的静态指纹特征，包括终端类型、操作系统、硬件与网络地址、安装应用、开放端口等；然后通过深度数据包检测和深度数据流检测，对终端的通信行为进行分析，提取应用访问的动态行为特征，包括流量曲线、安全现状、威胁等级等；在此基础上，利用特征工程、网络秩序流重构等方法，比如通过综合 SSL/TLS 握手过程和流统计的特征提取方法，提升采集的静态指纹和动态特征匹配的准确度[17]。

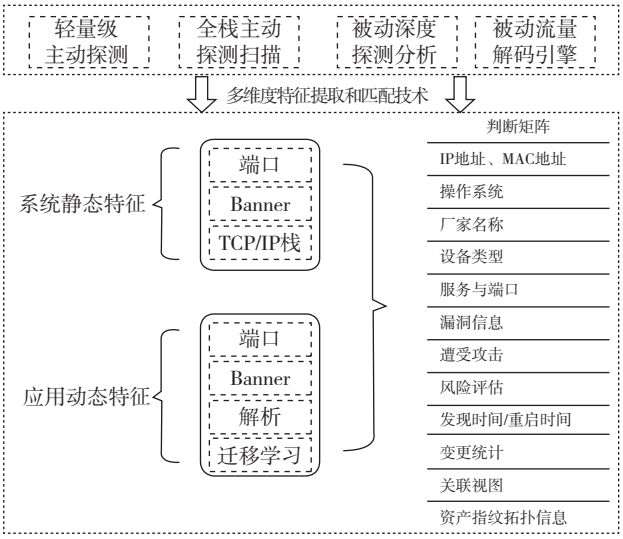

图 2　终端指纹提取与识别方法

另外，基于业务行为的终端身份要素提取需要从终端的所有业务访问数据中提取出有价值的特征值，例如频繁访问的端口、服务，访问频次的峰值、谷值，接口访问的平均频率等终端网络频域行为指纹、终端协议行为指纹。终端安全行为指纹的构建需要综合射频设备采集到的硬件指纹以及之前计算出的网络频域、终端协议指纹，业务流交互指纹等，将不同类型设备提取的指纹特征进行归一化处理，并基于状态转移概率矩阵，将终端的行为模式特征进行输入，构建异构智能终端设备的统一身份标志，并进行存储。当设备再次请求的时候，进行调取比对，并对每次的访问数据进行迭代计算，不断更新终端指纹。指纹构建架构如图 3 所示。

4.2　海量高并发工业业务交互行为持续信任评估技术

系统利用工业业务交互行为数据、硬件指纹数据进行终端的持续信任评估建模。主要涉及数据的采集、解析、特征提取、训练基准模型、信任度评估；同时，基于不断采集的数据对信任评估模型做持续的、及时的迭代调整。评估流程架构如图 4 所示。

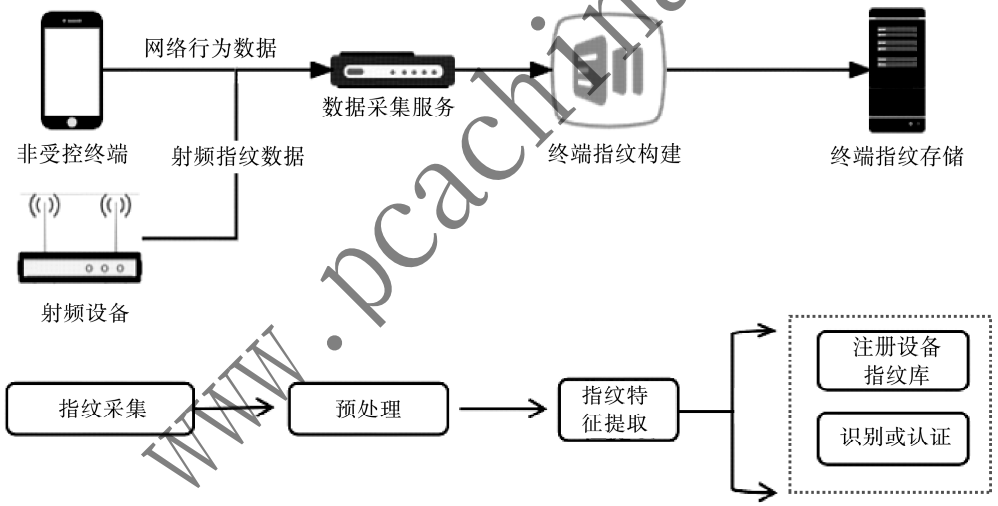

图 3　终端指纹构建架构图

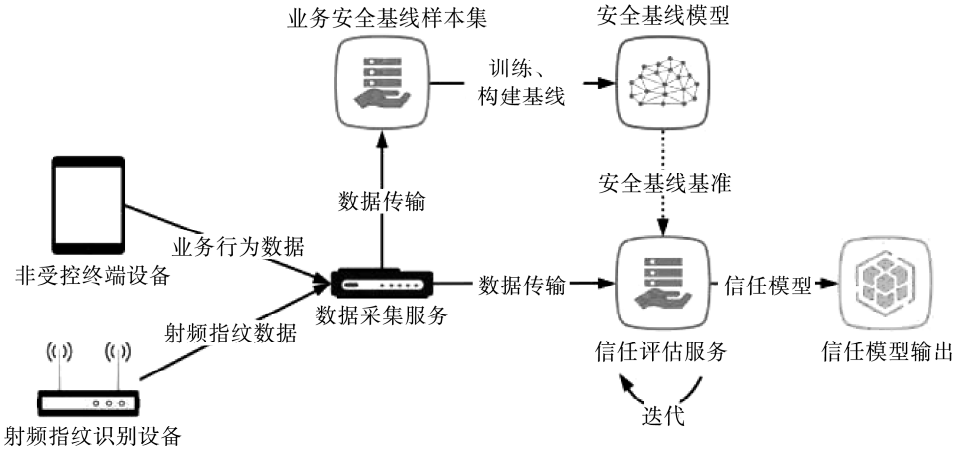

图 4　持续信任度评估架构

其中业务行为数据是各种工业终端访问业务系统时产生的交互流量数据，包括通信协议、端口访问、业务协议等数据；射频指纹数据主要是通过射频采集设备，构建接入终端的硬件指纹信息，用以标记终端身份。数据解析需要对捕获的数据包进行快速处理，主要是提取业务流量中的各种协议数据、端口数据、访问的业务 API 数据、访问时间数据等，同时解析硬件指纹，识别出具体非数控终端身份，明确设备对应关系。这些统计数据将作为后面特征提取的信息源。

为了在数据量较大的设备上实时提取和处理特征，特征集合的计算量不能过高，这限制了特征维度不能过高，而且需要从流级别进行快速的流量报头信息统计。基于采集的业务行为数据、硬件指纹数据，引入卷积神经网络等算法对业务交互行为进行深度学习分析，构建网络流量的空间、时间等特征矩阵模型。依据业务安全基线预设的频次异常、操作异常、流量异常、协议异常、模式异常、数值异常等偏差值，将业务终端进行分簇，计算当前终端的信任度，同时建立终端信任度的持续偏差分析，构建信任度曲线。

4.3　边缘安全防护微服务的动态访问控制技术

在工控网络边缘研究基于 SDN/NFV（软件定义网络/网络功能虚拟化）的安全防护微服务的动态访问控制方法，通过安全服务的灵活加载，实现边缘网关的动态访问控制能力增强；通过收集网络边缘的流量和用户行为，细粒度地识别攻击类型、攻击阶段，监测和识别物联网设备的安全风险，在此基础上，研制具备自适应、高效的设备异常行为分析及访问控制能力的边缘网关装置。通过安全微服务的灵活加载，提供虚拟防火墙、虚拟入侵防御、虚拟行为管理、虚拟流量控制等虚拟网络功能（Virtual Network Function，VNF），实现基于边缘网关的微服务隔离。将原先离散的、异构的设备形成统一的逻辑安全能力资源池，根据终端指纹特征、业务访问规则制定不同的访问控制策略，实现终端业务流安全服务的差异化处理，并可以通过模板化、可加载方式支持安全业务的灵活定义、按需部署、弹性扩展[18]。

5　系统应用

系统已成功应用于中核集团某厂矿工控网络的基于零信任的终端可控项目。方案的重点是非受控终端的接入管控，特别是对非授权访问、非法侵入及内外网透传等异常行为的检测，实现工控网络各类终端自动探测、合法验证和精细管控；提升终端接入的安全防护能力，防范利用网络末梢终端安全隐患攻击核心网络及关键系统的安全威胁；能够大幅增强终端准入控制和异常行为监测能力，确保终端接入的安全性，提升新型工业系统数字化建设全场景安全防护能力。组网部署方案如图 5 所示。系统采用二级部署，分别部署在管理信息大区、

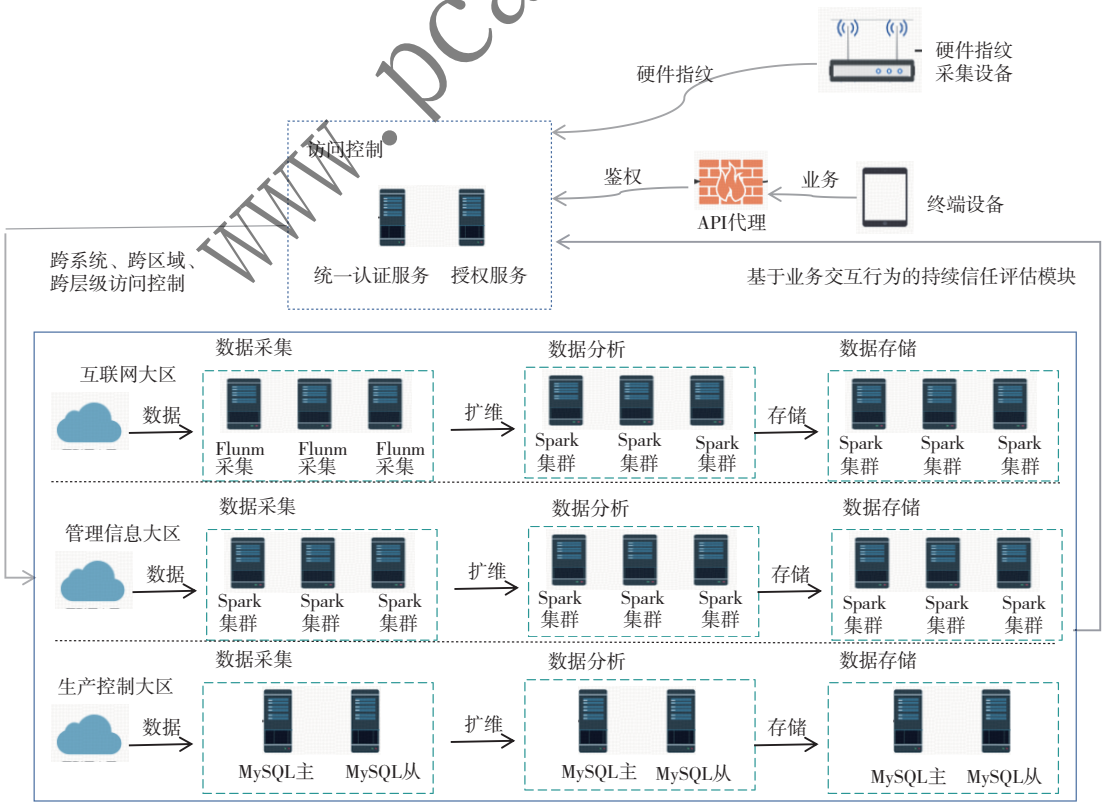

图 5　基于零信任的终端可控部署实施

生产控制大区和互联网大区内，通过数据同步服务，对各大区的终端指纹信息、信任度评估信息、访问控制权限信息进行实时同步共享，实现终端基于业务的跨网段、跨系统、跨层级的安全访问。

通过准入网关接入服务端，实现准入控制，对系统各类终端进行安全加固、资产管理、行为审计、分析展示等，并进行多维度风险综合评价，如图 6 所示。现场可以提供对 S7、Modbus-TCP、EtherNet/IP、PROFINET、OPC、DNP3 等协议流量统计与事件关联分析，既有针对工控指令攻击、非法设备接入、会话重用、攻击参数篡改、恶意代码等的攻击检测，也有针对误操作、PLC 下装、操作指令变更、违规行为、工程师站组态变更、I/O 信号阈值越界等异常工控事件的告警与记录，并通过回溯功能对海量异构数据的告警进行聚合分析、记录和存储。如图 7 所示，针对矿区重要的生产管控辅助系统，通过对数据包七元组会话特征分析与模型预警，提前发现规避了会话重用的重大安全隐患，并通过零信任网络安全架构持续信任评估、动态访问控制等功能，实现终端用户退出系统后，服务器端授权及时失效，显著减少网络风险暴露面，降低漏洞利用率，大幅提升工业终端接入业务系统的安全性。

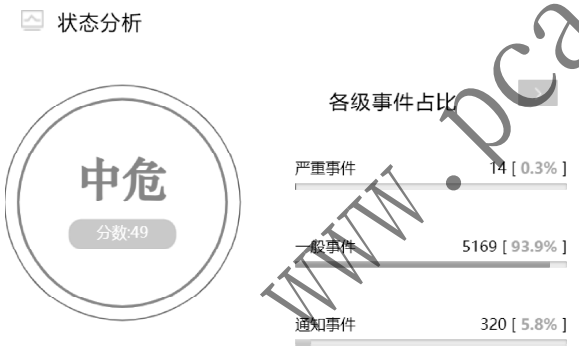

图 6　工控网络终端接入安全风险监控

资产厂商	资产分组	变更状态	安全状态	阻断
戴尔	17楼	有变更	中危	阻断
Hon Hai Precision I...	17楼	有变更	中危	阻断
威睿	17楼	有变更	中危	阻断
Universal Global Sc...	17楼	有变更	中危	阻断

图 7　重要业务系统的安全防护案例

6　结论

本文基于零信任安全防御架构，结合软件定义网络、网络资产探测、指纹信息采集构建、身份认证、访问控制、安全检测、信任度评估模型等物联网终端安全可信接入关键技术，形成新一代零信任安全防御机制，这种主动防御机制能够提高对任意威胁的抵御能力，有效防范新型业务应用与终端接入带来的安全风险，提升工业互联网安全防护体系的纵深防御能力。

参考文献

[1] 本刊记者. 国家工信安全发展研究中心发布《2022 年工业信息安全态势报告》[J]. 信息网络安全，2023，23（3）：106.

[2] 董悦，王志勤，田慧蓉，等. 工业互联网安全技术发展研究 [J]. 中国工程科学，2021，23（2）：65－73.

[3] 王泽鹏，马超，张壮壮，等. 动态决策驱动的工控网络数据要素威胁检测方法 [J]. 计算机研究与发展，2024，61（10）：2404－2416.

[4] DHAR S，BOSE I. Securing IoT devices using zero trust and blockchain [J]. Journal of Organizational Computing and Electronic Commerce，2021，31（1）：18－34.

[5] 安宇航，冯景瑜，庹善德，等. 工业互联网中抗 APT 窃取身份的零信任动态认证 [J]. 信息安全研究，2024，10（10）：928－936.

[6] 郭仲勇，刘扬，张宏元，等. 基于零信任架构的 IoT 设备身份认证机制研究 [J]. 信息技术与网络安全，2020，39（11）：23－30.

[7] 石进. 基于零信任机制的工控网络安全防御技术研究 [D]. 北京：华北电力大学（北京），2022.

[8] 张刘天，陈丹伟. 基于零信任的动态访问控制模型研究 [J]. 信息安全研究，2022，8（10）：1008－1017.

[9] 王群，袁泉，李馥娟，等. 零信任网络及其关键技术综述 [J]. 计算机应用，2023，43（4）：1142－1150.

[10] LI S，LQBAL M，SAXENA N. Future industry internet of things with zero-trust security [J]. Information Systems Frontiers，2024，26（5）：1653－1666.

[11] STAFFORD V A. Zero trust architecture [EB/OL]. [2024－09－30]. https：//nvlpubs. nist. gov/nistpubs/specialpublications/ NISTSP800－207. pdf.

[12] 冯景瑜，于婷婷，王梓莹，等. 电力物联场景下抗失陷终端威胁的边缘零信任模型 [J]. 计算机研究与发展，2022，59（5）：1120－1132.

[13] WANG Z，JIN M，JIANG L，et al，Secure access method of power Internet of Things based on zero trust architecture [C]// Proc. of Int. Conf. on Swarm Intelligence. Berlin：Springer，2023：386－399.

[14] 刘涛，马越，姜和芳，等. 基于零信任的工控网络安全防护架构研究 [J]. 工业信息与通信技术，2021，19（7）：25－32.

[15] 王航宇，吕飞，程裕亮，等. 工业物联网零信任安全研究

综述［J］. 计算机研究与发展，1－23［2025－03－01］. https：//link. cnki. net/urlid/11. 1777. tp. 20250407. 1652. 018.

［16］廖天颖，杨斯博，窦润亮. 基于贝叶斯网络的大数据安全动态风险评估模型研究［J］. 网络空间安全，2023，14（1）：60－68.

［17］曾彬，王雷，文吉刚，等. 智能物联终端安全可信接入关键技术研究［J］. 长沙大学学报，2022，36（5）：9－14，23.

［18］施海滨，钟祝君. 基于 SDN 和 NFV 的云安全体系建设［J］. 中国金融电脑，2015（11）：26－28.

（收稿日期：2025－03－06）

作者简介：

孙国锋（1980－），男，本科，工程师，主要研究方向：工业互联网系统架构与安全运维。

曾彬（1979－），男，博士，高级工程师，主要研究方向：AI 与大数据分析技术在复杂网络中的应用。

唐宁（1983－），男，大专，主要研究方向：工控系统安全运维。

“生成式人工智能安全”主题专栏征稿启事

生成式人工智能（GenAI）在内容创作、医疗诊断、金融分析等领域展现巨大潜力，正以前所未有的速度重塑我们的生产、生活与认知方式。然而，其迅猛发展也伴随着复杂严峻的安全挑战，从深度伪造操纵舆论、模型生成内容侵犯知识产权，到数据投毒攻击误导决策、隐私泄露引发伦理危机，GenAI 的安全问题受到广泛关注。

为此，《网络安全与数据治理》拟在 2025 年第 11 期推出“生成式人工智能安全”主题专栏，旨在汇聚行业智慧，共同应对 GenAI 发展带来的安全挑战，推动安全、可靠、可信的生成式人工智能发展，现诚挚邀请相关领域的专家学者、科研人员踊跃投稿！

一、征文主题：生成式人工智能安全

包括但不限于以下学术方向：

1. 对抗攻击与防御；
2. 内容安全与滥用防控；
3. 隐私保护技术；
4. 数据投毒攻击与防御；
5. 数据溯源与知识产权保护；
6. 模型可靠性研究；
7. 安全评估指标和标准研究；
8. 监管政策与法律规范研究。

二、投稿要求

1. 稿件请用 word 格式录入，并套用本刊投稿模板。模板下载网址：http：//files. chinaaet. com/files/Periodical/pcachina_ Templates. doc

2. 投稿文章须未在其他期刊或者出版正式论文集的会议上刊登过，且不在其他刊物或会议的审稿过程中，不存在一稿多投现象。

3. 保证文章的合法性（无抄袭、剽窃、侵权、虚假引用等不良学术行为），且不违反相关法律法规，不涉及国家、企业秘密，稿件文责自负。

4. 论文要求观点鲜明、逻辑严谨、论据充分、方法合理，字数在 5000～8000 字。

5. 请在官方投稿网站（http：//www. pcachina. com）注册、投稿。注册后请投稿在“人工智能”栏目。稿件经评审合格录用后，在《网络安全与数据治理》2025 年第 11 期（正刊）以主题专栏形式发表。

三、专栏主编

于静

中央民族大学信息工程学院，博士，副教授

赵悦

中央民族大学，博士，教授

盖珂珂

北京理工大学人工智能学院，副院长，教授，博士生导师

四、时间安排

截稿日期：2025 年 10 月 10 日

出刊日期：2025 年 11 月 15 日

《网络安全与数据治理》编辑部

2025 年 7 月

版权声明

凡《网络安全与数据治理》录用的文章，如作者没有关于汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权等版权的特殊声明，即视作该文章署名作者同意将该文章的汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权授予本刊，本刊有权授权本刊合作数据库、合作媒体等合作伙伴使用。同时，本刊支付的稿酬已包含上述使用的费用，特此声明。

《网络安全与数据治理》编辑部