中数国科工控网络安全审计系统

产品白皮书

（北京中数国科技术股份有限公司）

【中数国科】

■ 文档编号	■ 密　　级
■ 版本编号	■ 日　　期
■ 撰 写 人	■ 批 准 人

变更记录

序号	版本	变更记录	修改人/日期	检查人/日期	审批人/日期
1					

目录

1 背景概述

当前，80%以上的关键基础设施（能源、石油化工、交通、市政等）都依靠建立在工业网络之上的自动化监控系统来实现自动化生产作业和运营。工业控制系统被誉为关键基础设施的大脑和神经网络，工业控制系统的安全可靠关系到关键基础设施安全运行，关系到国家安全。

随着两化融合的快速发展，工业控制系统也不断引入最新的计算机及网络技术来提高系统的集成度、互联互通以及海量信息处理能力。未来节能环保、消费升级及市场竞争加剧等因素的进一步驱动，关键基础设施相关的工控网络会越来越开放互联，由此带来的网络安全风险成为当务之急。传统的信息安全防护产品及措施无法满足工业控制网络的安全需求。

工业控制系统的网络及联网设施被攻击，可能破坏企业重要装置的正常工艺流程，由此引发的后果是灾难性的。国家对工业控制领域的安全问题也极其重视。2016 年 10 月，工业和信息化部印发《工业控制系统信息安全防护指南》，明确了在工业控制系统网络中部署网络安全监测设备，以便及时发现、报告并处理网络攻击或异常行为。2017 年 10 月《信息安全技术 网络安全等级保护安全设计技术要求》(等保 2.0)通用技术要求明确提出，应在网络边界、重要网络节点进行安全审计， 审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计。2017 年 6 月 1 日，《中华人民共和国网络安全法》正式施行，在国家层面，对于工业控制系统的安全风险越来越重视。

由于工业控制领域的特殊性，传统企业 IT 网络应用的 IT 网络监测审计产品、主机监测审计产品、数据库监测审计产品及各种应用监测审计产品在物理环境、网络环境、适用场景等方面与工业控制网络及其主机、数据库和各种工业生产监测控制专用应用的审计需求均有很大的差异，IT 网络安全审计产品因缺乏对工控协议的解析能力而不能直接用于工业控制网络中，同时现有的工业控制网络缺乏对用户操作、工控网络行为、指令下发等的审计措施，导致安全事故分析取证困难。另外， 部分工业控制网络相关产品不具备审计功能或者虽有日志审计功能但系统的性能要求决定了它不能开启审计功能。所以传统企业/IT 网络应用的监测审计产品在工业控制网络环境中并不适用。

中数国科的产品和技术团队通过对工业控制系统及其网络多年的深入研究理解和工控网络安全服务实践，结合工业现场实际生产工艺流程、生产环境特殊性，设计开发了符合工业现场应用的 ISA 系列工业网络监测审计系统产品，帮助客户加强和提升工业控制网络的安全审计能力。ISA 系列工控网络安全审系统，通过内置的多种漏洞特征库及智能算法的高速解析引擎，对工业网络镜像流量数据进行深度解析，对报文深度解析和智能关联分析，实现对工业控制网络的异常行为、协议攻击、关键事件进行实时检测，对异常工业报文、异常操作行为、异常访问及恶意攻击等进行及时告警，实现多种安全风险的监测分析和预警，确保工业网络安全可靠运行。及时发现外部攻击事件、内部违规事件等，为安全事故/故障调查分析提供详实的记录。

ISA 系列工控网络安全审系统产品软件通过采用流量高速捕获引擎、智能冗余算法等提高网络审计效率，硬件采用冗余设计及选用工业级器件和严苛测试等，数据接口及通讯采用加密，使系统自身安全性和可靠性得到有效保障。

ISA 系列工控网络安全审系统，可配合工业防火墙、工业网闸等一起使用，从而有效补充工业防火墙的不足，完成对工业控制网络安全事件和异常流量行为的完整追溯还原。工控网络安全审系统可自管理，也可接入集中管理平台，通过集中统一安全管理平台进行集中管理和统一策略下发，进而构筑完善的工业网络安全防护体系。

2 产品概述

ISA 系列工控网络安全审系统是中数国科在对工控网络安全的深入理解和实践中打造的一款适用于工业控制网络信息安全实时监测的网络安全审计产品。采用旁路部署模式，无扰接入，对工业生产过程“零风险”。

ISA 系列工业监测审计平台搭载中数国科自主开发的 DPI/DFI 深度解析引擎，可对工控协议深度做到指令级的监测与审计，针对工控网络安全及指令行为安全提供坚实的基础。

ISA 系列工控网络安全审系统能实时监测工控网络/工控指令的行为和状态，检测工控网络中的入侵行为、流量异常，也能根据用户定义、白+黑名单、关联

预判等组合审计策略，追踪溯源工控网络安全事件。基于对适配工控网络的协议的通信报文进行深度解析（DPI，Deep Packet Inspection），能够实时检测针对工业协议的网络攻击、用户误操作、用户违规操作、未知设备接入以及异常报文、异常连接、蠕虫、病毒等利用资产漏洞进行恶意传播和破坏的行为，并实时告警，同时完整记录网络通信过程，包括工业控制协议会话记录，为工业控制系统的安全事故调查提供坚实的基础。

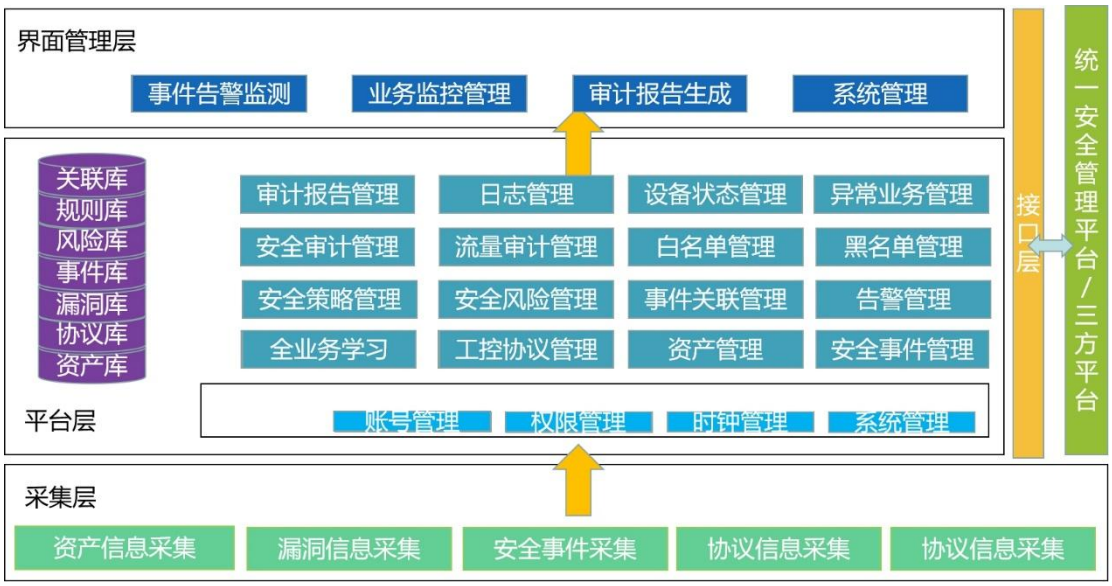
ISA 系列工控网络安全审系统适用于大中型 SCADA、DCS、MES、BAS、FAS、FCS、PCS 等工业控制系统网络，实现对 DCS、PLC、RTU 等分布设备的保护。

ISA 系列工控网络安全审系统可以被广泛的应用到石油石化、天然气、电力、钢铁、智能制造、水利、烟草、高速铁路、城市轨道交通、城市市政等行业以及其他与国计民生紧密相关领域的工业控制系统。

ISA 系列工控网络安全审系统有导轨式和机架式，导轨式产品满足 35MM 标准工业导轨安装，可方便地安装部署在生产车间/工控现场环境的导轨上而无需用螺丝固定， 维护方便；机架式设备可以部署在工厂或大型系统控制中心/车站等的机房标准机柜/机架上。

3 产品技术原理

ISA 系列工控网络安全审系统架构主要由采集层、平台层、界面管理层、接口层四部分组成，集协议识别、漏洞判别、安全事件、安全审计于一身，架构体系如下：



数据采集层：主要负责将工控网络中资产信息、漏洞信息、安全事件等各威胁原始信息镜像采集到系统采集层，由采集层采用主动智能学习引擎，做初始解析预判，根据确定信息进行分类存储，为后续深度关联判断作为依据。

采集层实时获得当前工控网络内主机设备、PLC、DCS、SCADA、网络设备、安全设备的流量信息，基于工控协议及 IT 网络协议、应用端口等信息对网络设备及应用等指标进行监控，从而实时获得工控网内安全威胁及各系统发送指令频率，为后续安全分析提供基础数据。

平台层：平台层作为工控网络安全审系统的核心层，囊括工控协议识别子系统，资产管理子系统、安全事件管理子系统、安全风险管理子系统、白+黑管理子系统、安全关联审计子系统、安全审计管理子系统、数据库等，为工控网络安全提供坚实后盾。

数据采集解析后，将数据投送 DPI 引擎，进行全量解析，匹配协议库、漏洞库、恶意程序库、攻击库等，实时准确判断工控网络中的各安全事件分类及关联关系性，根据多种安全策略提供告警机制，以邮件或界面显示的形式通知到对应管理人员，人工的判断及事件回溯。

工控网络安全审系统采用“零拷贝”并支持 IP 分片重组和 TCP 分段还原重组，高效准确的识别工控协议及支持工业畸形报文预警，为安全事件的事前、事后提供依据，监测审计系统支持 24 种主流工控协议，并能准确识别协议 OPCUA 和 OPCDA，在识别准确率上领先于同行业产品。

界面管理层：操作员通过统一的管理界面实现对工控网络资源的全面安全管理。根据智能学习结果，制定自身企业的对应安全策略，实现相应的告警机制。操作人员可实时了解生产网内事件告警、安全趋势、安全级别情况及趋势。通过信息可视化，将大量的安全信息以图 表、事件图的方式呈现出来，实现了监测审计系统自身及安全事件的全面审计，提升了全网安全监测的效率。

4 产品功能

4.1智能学习

工业审计平台基于智能规则学习引擎技术，可人为控制学习节奏，在审计系统初级部署对工控网络进行智能学习至协议、行为、流量不再变化，提取并建立网内的资产、协议和流量规则及基本特征，工业企业可根据自身设备及网络环境特点分析判断部署归属到白名单或黑名单，依据网内资产、协议白名单、黑名单、安全事件、系统事件，后续关联预判等策略，为持续审计做好基础准备。

4.2实时工业网络安全监测

默认交换机镜像数据旁路接入的方式对工控网络进行实时监测，基于白+黑名单，协议安全规则，对协议、流量、日期和时间、资产、事件类型、风险、协议指令等元素实时进行监测审计并进行统计分析，应激显示网络的安全状态并产生告警状态。

4.3资产管理

工业审计平台部署初期可通过智能学习技术，自动识别流量中的资产信息并归属至资产白名单中，作为资产基线并作为后续资产安全判断的重要依据。

工业审计平台可实时自动的识别流量中的资产信息并自动收录，识别后归属为未知设备，可显示设备名称、制造厂商、首次出现时间、最后出现时间、IP 地址、MAC 地址等信息，操作员可根据企业内实际环境及管理政策可决定是否收录至资产白名单中或不允许出现在生产环境中。

工业审计平台可实现手动录入资产信息，并添加至资产白名单中，同时在资产白名单中可实现 IP 地址与 MAC 地址绑定,达到固化资产的目的，当出现地址盗用时，审计平台持续监测网络中存在的设备 IP 地址盗用的行为并进行告警提示。

4.4工控协议深度检测和流还原

深度监测引擎采用零拷贝技术，支持 ip 分片重组和 TCP 分段还原重组，最大的提升识别速率及准确率，支持工业畸形报文预警。工业审计平台基于深度监测引擎解析工控协议通信行为的过程，通过白名单机制构建工控协议的通信行为建立模型。

深度数据包解析引擎支持包括 Modbus TCP、 IEC104、 DNP3、S7、CIP、Ethernet/IP、 OPC 等在内的 24 种大多数企业主流工控协议，同时支持自定义协议设置，协议库与自定义协议相结合的方式，深度检测工业协议的指令集和数据报文的流还原，为安全事后追踪提供依据。

4.5自定义协议

工控网络安全审系统支持自定义协议，用户可根据实际情况，修改编辑自定义协议规则文件，实现特定协议的深度解析和审计支持。

4.6入侵监测

通过分析工控网络通信，建立通信关系图，采用 DPI 和 DFI 技术对流量进行提取深层分析，分析建立特征指纹库，对工控网络入侵进行实时检测分析，利用内置的工控漏洞库和工控行为白名单建立监测规则，对缓冲区溢出、SQL 注入、暴力猜测、DDoS 攻击、扫描探测、蠕虫病毒、木马后门等各类黑客攻击和恶意流量进行实时检测及告警。

4.7内网主机异常通信监测

采用智能边界技术，实时监测内网主机非法外联、内网主机异常连接行为，发现异常通信记录，并实时向管理平台或态势感知进行告警。

4.8异常报文监测

实时检测报文的完整性，可对异常数据包报文，及时发现并产生告警。记录异常报文事件。

4.9无流量监测

可根据实际业务灵活配置协议无流量监测行为，可针对各个协议设置无流量认定时长，对多种协议进行持续无流量监测审计，及时发现工业通讯中断的异常工况并上报相应时间告警。

4.10 不合规行为监测

通过自定义规则或白名单规则，检测业务流量中不合规的工控网络行为，对不合规行为进行实时的告警和响应，留存网络数据。

4.11 通信关系画像

工控网络安全审系统支持通信关系画像，可直观呈现端对端的通信交互行为关系。画像提供直观易用的界面，快速呈现资产之间的可信业务通信交互、违规连接通信交互、高风险的非法外联通信交互关系。通信关系画像支持数据钻取和分级显示，能够显示到流级别，方便快速定位端对端的通信行为详情，包括协议和会话详情。

4.12 数据留存

根据用户自定义设置，留存所有网络的原始数据，可配置为留存六个月及以上时间。

4.13 报表

工控网络安全审系统提供强大的报表功能。报表支持按条件统计生成，报表

包括：概览、资产审计、网络审计、安全事件、协议分析、流量分析等模块。报表支持时间段定制、Web 查看，支持 PDF 格式导出。

4.14 系统自身安全性

基于 SSL 的远程管理：通过网络可以直接对工业监测审计产品进行管理和配置。通讯采用了 SSL 加密技术，所有配置管理信息在网络上全部以密文传输，可以防止恶意攻击者使用网络监听工具窃取信息。

基于角色的分权分级管理，有利于减少对系统的滥用。

4.15 安全审计及异常响应

对安全事件进行审计，及时追溯安全事件的轨迹。

对用户的操作行为进行细粒度审计，方便还原操作的真相。

独立的告警响应机制，可定义对不同安全级别的安全事件的响应方式。

5 产品优势

5.1健全的系统部署和管理能力

系统采用旁路部署模式，通过流量镜像的方式对工控网络进行全流量数据监测，做到对工控网络“无感知，零风险”，同时具备单一设备自管理，也可以进行集中管理，满足不同工业网络支撑环境的部署需求。

5.2多种组合监测机制

通过“白名单+黑名单+关联机制”策略构建多重检测机制，准确识别不合规操作等异常通信行为，并产生告警。采用以下手段对于应对日益严重的 APT（高级可持续性威胁）攻击提供了防护：

1）支持对已知攻击行为的检测和防护，内置了庞大可升级的工控威胁库；

2）支持自学习工控协议规则和行为，建立安全检测模型；

3）可通过白名单和黑名单防护阻止不明的威胁；

4）针对模糊行为，可通过制定关联分析多组合策略，建立安全模糊攻击检测模型；

5.3用户可扩展的未知工业协议定制

工控网络安全审系统支持添加自定义协议，实现多种协议和协议扩展支持，满足特定工业网络场景的应用。

5.4实时告警

通过对工控网络协议的深度解析，对异常数据，重大控制事件，行为异常等不符合工控安全行为的事件实时告警。

5.5画像和数据钻取

工控网络安全审系统支持通信关系画像，直观呈现端对端的通信交互行为关系， 通过数据钻取，能够逐级探查通信协议和会话详情。

5.6工控协议无流量检测

工控网络安全审系统支持工业协议及 IT 协议无流量检测功能，可持续监测全局流量，学习工业协议的正常标准通信状态，设置无流量阈值，针对突破无流量阈值的异常中断事件进行实时报警。

5.7工业级硬件设计

产品硬件采用了适应工业环境的硬件设计。

➢ 防护等级 IP40，满足工控网络应用环境要求。

➢ 通过多项安全认证、可靠性和稳定性满足要求。

➢ 通过工业级宽温测试，工作温度、湿度、满足工业现场要求。

➢ 低功耗、无风扇、全封闭设计。

6 产品价值

(1) 合规性价值

符合国家安全性政策法规，满足对网络边界、重要网络节点进行安全审计；

审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；

可对工控网络的原始数据进行加密存储，审计数据可留存六个月及以上时间，满足等级保护 2.0、网络安全法以及行业相关的合规性要求。

(2) 安全追溯，事件溯源取证

细粒度的监测和审计能力，解决安全实时性预警外，提供有效的事件还原能力，增强事后分析调查取证能力，规避工控系统持续受损。

(3) 安全风险，发现及时性

威胁及早发现，避免重大损失。通过工控网络安全审系统实时的检测和审计，及时发现网络风险，提早介入网络治理，避免网络和关键设施停机风险。

(4) 安全事件可视性

可视化展现工控网络的通信行为和安全状况，方便安全管理人员快速、准确地定位安全事件，提高企业工控网络安全管理效率。