天融信工控安全监测审计系统TopIAS（NG系列）

www.topsec.com.cn

产品概述

天融信工控安全监测审计系统（TopIAS）是一款专门针对工业控制网络进行行为分析和安全监测的审计类产品。系统集工业协议解析、工业行为审计、工业流量审计、工业资产发现、威胁实时展示等核心功能于一体，可有效针对工业控制系统的异常攻击、异常流量、违规操作、误操作、非法指令等异常行为进行实时监测与审计，并对安全事件详情进行记录和报文留存，为安全事件调查提供基础依据。帮助工业企业实时掌握生产网运行情况，持续监测安全风险。

产品特点

全面的工艺行为审计

系统可有效针对工业控制系统通讯内容的写操作、读写范围、值范围等工艺行为审计与分析。解决针对误操作、非法操作、组态变更、负载变更、操控指令变更、PLC下装等破坏行为不能被精确识别问题。

深度的协议解析技术

系统内嵌工控协议深度解析引擎，支持Modbus、IEC104、EIP、OPC-UA、OPC-DA、S7、DNP3、IEC61850-MMS、Profinet等工控协议的识别和深度解析；包括对数据包完整性、功能码、地址范围、值范围、变化趋势等多层次的深度解析，及时发现违规操作、异常指令等安全威胁。

多维度安全行为基线

系统采用深度自学习技术，通过流量分析建立基于会话、流量、指令、资产等多个维度的安全检测基线。有效检测恶意攻击、非法接入和误操作等违规行为，生成多样化的告警。帮助客户实时掌握网络中的运行状态，发现潜在安全威胁。

高效的工业资产管理

系统采用资产自动匹配技术，发现数据包中的特殊字段或者指纹特征，有效识别资产的IP地址、协议、端口、厂家信息、型号、版本等信息，分析资产关系，自动生成资产拓扑，建立起完整的工业资产台账，帮助客户彻底摸清家底。

精准的事件溯源技术

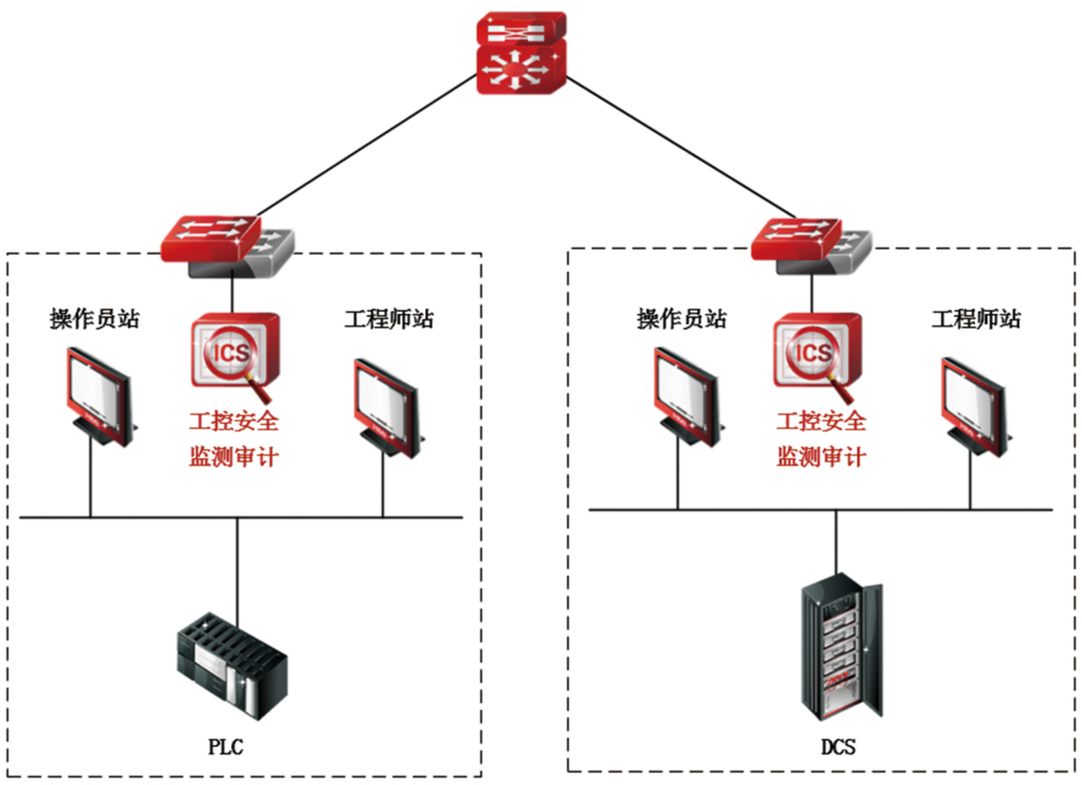
系统依托协议深度解析技术，可完整还原工业现场通讯过程，记录工业网络的所有操作行为、网络会话、异常告警等安全日志。同时支持事件录播功能，可留存安全事件发生时刻前后一段时间内的报文信息，为相关机构调查取证和回溯分析提供基础依据。

可靠的工业硬件设计

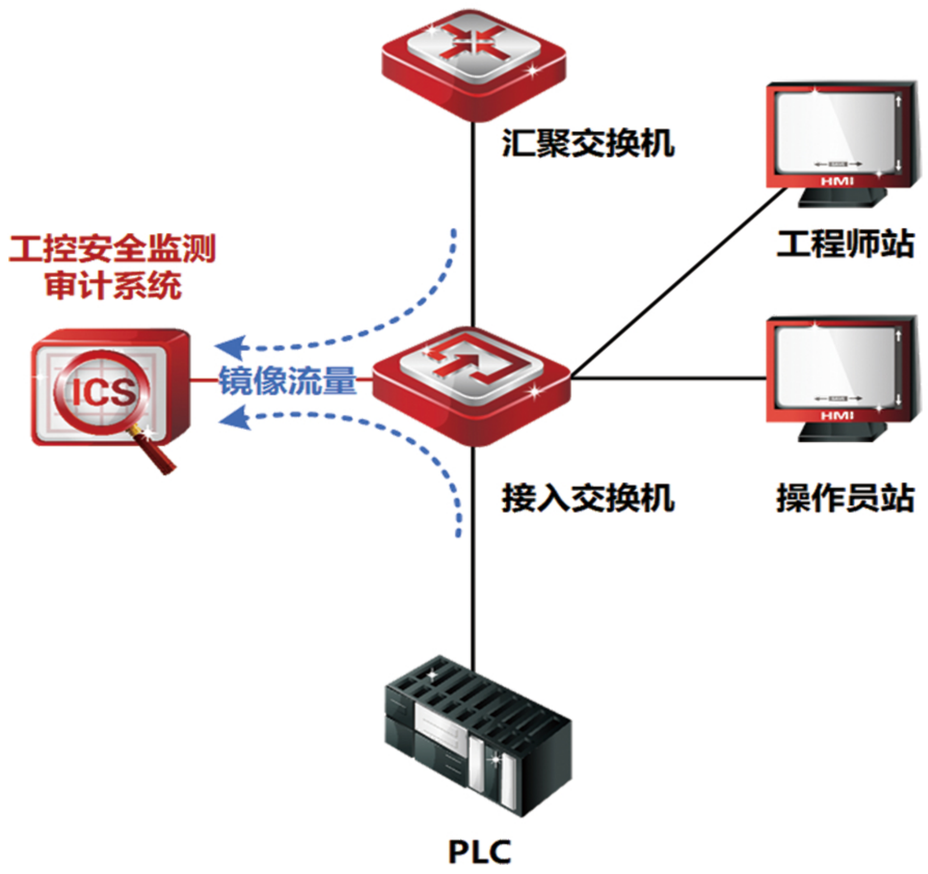
硬件平台设计遵循工业标准，采用高性能工业级处理器、无风扇、电源冗余、铝合金全封闭设计，硬件平台达到IP40防护等级，能够满足工业环境下宽温、防尘、防潮、防盐雾和高可靠性要求，支持导轨式、机柜式安装等多种安装方式。

典型应用

依据业务功能特点，对生产网络划分安全区、安全域，将工控安全监测审计系统旁路部署在生产网络各个区域的汇聚层交换机上，通过镜像方式将数据流量发送到工控安全监测审计系统上进行统计分析，一方面对各个业务子系统操作员站、PLC的异常通信、违规操作、协议规约异常以及关键事件（如寄存器读写操作）等进行告警、记录分析；另一方面，对来自其他网络的异常操作、异常通信、违规操作等进行告警记录，及时采取防范措施。



工控安全监测审计系统采用旁路方式部署于关键业务系统前端，被动接收工控业务流量，通过特定的白名单审计策略，对控制网内部的通讯行为进行逐个比对，包括数据包的完整性、功能码、地址范围、值范围和变化趋势等，发现超出白名单策略的通讯行为，并及时告警和记录安全事件通讯过程，实现关键系统的监测与审计工作。



客户价值

技术自主可控，降低后门安全风险

天融信工控安全团队拥有国内成熟可靠的软硬件安全研发技术，产品采用工业级硬件平台和专有的安全操作系统NGTOS进行设计，提高整体方案中各组成部分的安全性，杜绝大量非自主可控技术带来的安全漏洞隐患。

及时发现风险，避免安全事故发生

天融信工控安全监测审计系统结合工业环境实际业务特点，制定安全检测策略，及时发现异常通信、误操作、违规操作、非法设备接入等安全威胁，统一上报安全管理平台，制定主动防御策略，实现联动防御部署，避免发生安全事故。

威胁可视化展示，提高安全审计效率

天融信工控安全监测审计系统支持工控网络资产自动梳理功能，可提供直观、清晰的网络拓扑和异常信息列表，真正解决工业控制系统黑箱问题，协助用户了解网络运行状况，轻松掌握网络异常趋势。

响应国家政策，满足行业合规性要求

天融信工控安全监测审计系统软硬件均按照国家和多个行业标准设计研发，可满足不同行业对于安全防护相关政策法规要求。例如《信息安全技术网络安全等级保护基本要求》（GB/T 22239-2019）、《工业控制系统信息安全防护指南》（工信软函〔2016〕338号）、《关于加强工业控制系统信息安全管理的通知》（工信部〔2011〕451号）等。