产品概述

恩创工控安全监测与审计系统是专门针对工业控制网络的信息安全审计平台，采用旁路模式部署，对工业生产过程“零风险”。基于对工业控制协议（如OPC、Siemens S7、Modbus TCP、Ethernet/IP（CIP）、IEC61850 MMS、IEC104、DNP3、Profinet、OMRON Fins等）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、非法设备接入以及蠕虫、病毒等恶意软件的传播并实时报警，同时详实记录一切网络通信行为，包括指令级的工业控制协议通信记录，为工业控制系统的安全事故调查提供坚实的基础。

产品特点

基于DPI的工控协议深度解析

识别100多种工业协议，提供主流工业协议的深度报文解析，有效识别协议动态端口，提供报文格式检查，完整性检查，指令检查等功能，支持OPC、Modbus TCP等十余种主流工控协议支持超过1000种的功能码识别。

细粒度协议指令与监测

通过工控协议的深度解析能力，结合“白名单+智能学习”机制，对各类工控协议数据包进行快速捕获和指令级解析。利用智能算法学习建立工控通信基线，对网络中工控协议通信行为与基线进行对比分析，不符合工控通信基线的异常指令操作、新设备（IP地址）、异常连接行为、异常通信地址/端口等将触发告警。

工业环境硬件设计

硬件平台设计遵循工业标准，采用高性能工业级ARM处理器（注：SMA 5600系列），无风扇设计，关键部件冗余设计，硬件平台达到工业三级B以上指标，能够满足工业环境下宽温、防尘、防潮和高可靠性要求，支持导轨安装、壁挂式、机柜安装等多种安装方式。

支持私有工控协议开发定制

产品内置工业协议解码引擎，提供软件SDK开发工具包，可基于协议语言描述规范自行定义私有协议，支持私有工控协议定制化二次开发。

功能规格

工业协议深度解析

- 支持OPC、Modbus、IEC 60870-5-104、IEC 61850 MMS、Siemens S7、Ethernet/IP（CIP）、DNP3、Profinet、Fins等主流工控协议解析
- 支持1000多种协议功能码识别
- 支持OPC DA，HAD，A&E，DX，XML-DA等操作，包括支持OPC的动态端口、OPC只读等；
- 支持Modbus TCP协议语法检查、Reset及连接跟踪、协议白名单，点表等；
- 支持ModBus、OPC协议值域控制；
- 支持Siemens S7协议读写操作、版本号、寄存器区、DB区区号、点类型、值范围、传输层协议控制等；
- 支持Ethernet/IP(CIP)协议语法检查及丢包Reset，支持Ethernet/IP(CIP)协议本身自定义的参数配置，支持CIP数据表、PCCC控制；
- 支持对Profinet协议传输功能码及操作对象进行控制；
- 支持IEC104协议白名单、传输原因长度、公共地址长度、信息体地址长度等的配置
- 支持DNP3协议白名单，包括版本号、源IP、目的IP、源IP掩码、目的IP掩码、源地址、目的地址、功能码、对象组号、变体号、传输层协议；

事件告警

- 支持对工控协议报文不符合其规约规定的格式进行检测并告警；
- 支持对工程师站组态变更、操控指令变更、PLC下装、负载变更等关键事件告警；
- 支持对告警事件一键加入白名单；
- 支持关键服务中断检测，在设定的时间内，单IP 某服务的接收报文为零时进行告警；
- 支持允许管理员自定义工控协议通信告警规则，对符合告警规则的通信行为进行告警；

协议通信记录

- 支持对所有网络会话信息的记录，并可通过规则设置进行调整记录信息；
- 记录主流工控协议的通信日志；
- 对非工控协议能够记录网络连接信息

正常通信行为建模

- 支持管理员对建立的工控通信模型白名单进行人工调校；
- 支持对当前通信行为与白名单进行对比，对偏离白名单的行为进行告警

异常流量监测

- 监测设备的流入流出流量并设置基线值，超出基线值进行报警
- 监测并采集系统内正常的网络通信，并可手动调校相关通信连接基线，对偏离基线的行为进行检测告警

事件分析统计

- 图形化显示一定时间段监控范围内的所有网络连接，并对异常的网络连接标记显示；
- 提供网络流量及报文数量的实时、历史分时、历史分天（可自定义范围）等的统计情况；
- 支持对各类告警事件进行多维度的统计

安全管理

- 通过IP认证、IP + MAC绑定的可信主机才能访问目前设备系统；
- 支持强制口令强度；
- 支持分权分级管理；
- 支持报表功能，用户通过报表可查看事件、日志和审计的统计数据，支持报表下载；
- 支持安全产品的自动升级

产品规格

导轨式



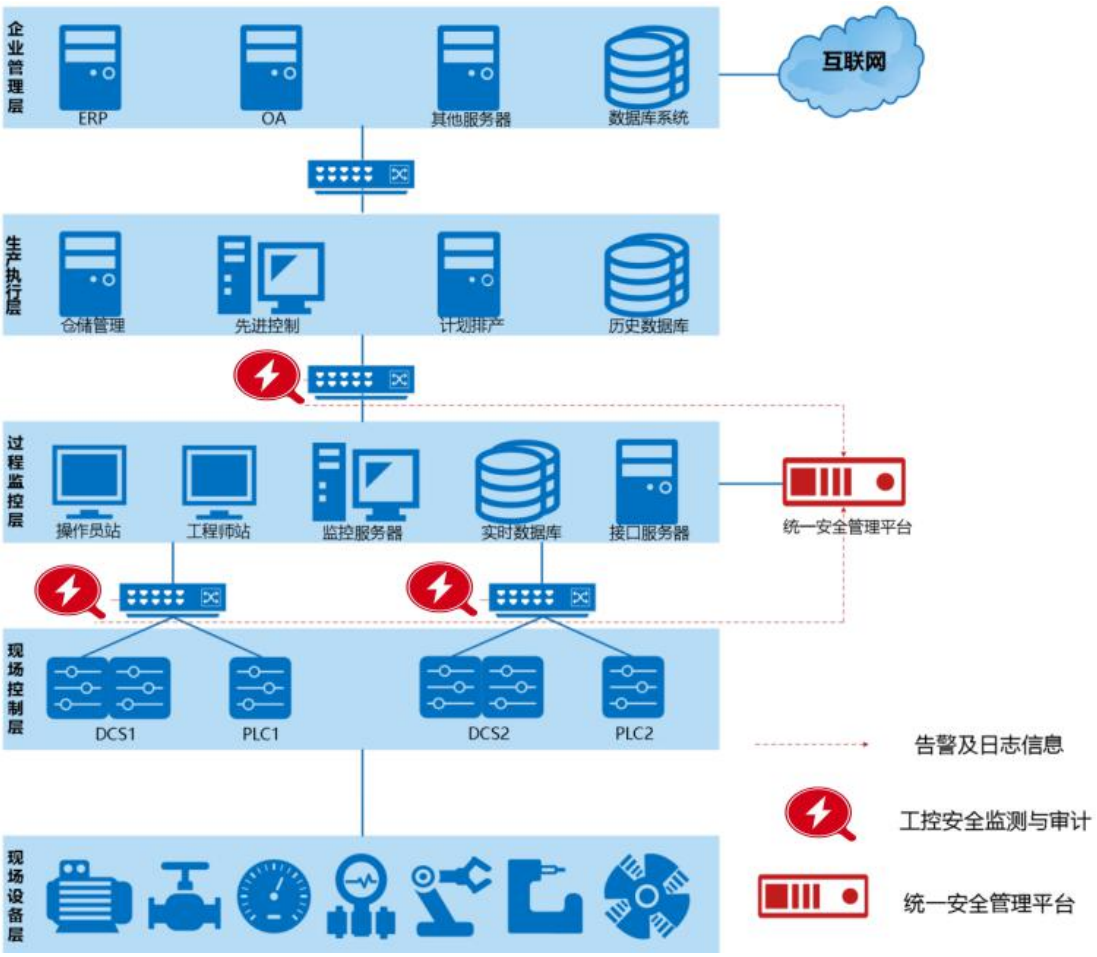
指标项	A1100	A2100	A3100
业务端口	2个千兆电口+2个千兆SFP口	4 个千兆电口	6 个千兆光电互斥接口
带外管理口	1个10/100/1000M自适应 RJ45口	1个10/100/1000M自适应 RJ45口	1个10/100/1000M自适应 RJ45口
Console 口	1个RJ45接口	1个RJ45接口	1个RJ45接口
串行接口	/	/	2个RS485、422、232自适应串口
USB 接口	1 端 口 USB 2.0	1 端 口 USB 2.0	1 端 口 USB 3.0
工作环境	温度：-40～75℃ 湿度：5%-95% 无凝结	温度：-40～75℃ 湿度：5%-95% 无凝结	温度：-40～75℃ 湿度：5%-95% 无凝结
存储环境	温度：-40～85℃ 湿度：5%-95% 无凝结	温度：-40～85℃ 湿度：5%-95% 无凝结	温度：-40～85℃ 湿度：5%-95% 无凝结
MTBF	25 万小时	25 万小时	25 万小时
电源	12-36V DC，冗余供电	12-36V DC，冗余供电	9-36V DC，冗余供电
最高功率	<7W	<7W	<14W
尺寸（宽*深*高）	58x118x168mm	58x118x168mm	89x150x135mm
安装方式	35mm 标准 DIN 导轨卡接	35mm 标准 DIN 导轨卡接	35mm DIN 导轨卡接安装 壁挂式安装

硬件指标



指标项	A2106	A2112	A2124
业务端口	6 个千兆光电互斥接口	8 个千兆电口+4 个千兆光电互斥接口	16 个千兆电口+6 个千兆光电互斥接口+2 个万兆 SFP+接口
带外管理口	1 个 10/100/1000M 自适应 RJ45 口	1 个 10/100/1000M 自适应 RJ45 口	1 个 10/100/1000M 自适应 RJ45 口
console 口	1 个 RJ45 接口	1 个 RJ45 接口	1 个RJ45 接口
HA 接口	/	1 个 10/100/1000M 自适应 RJ45 口	1 个 10/100/1000M 自适应 RJ45 口
串行接口	/	2 个 RS485/422/232自适应串口	2 个 RS485/422/232自适应串口
USB 接口	1 端 口 USB 2.0	1 端 口 USB 3.0	1 端 口 USB 3.0
工作环境	温度：0～40℃ 湿度：20%-80%，无凝结	温度：-10～60℃ 湿度：5%-95% 无凝结	温度：-10～60℃ 湿度：5%-95% 无凝结
存储环境	温度：0～40℃ 湿度：20%-80%，无凝结	温度：-40～85℃ 湿度：5%-95% 无凝结	温度：-40～85℃ 湿度：5%-95% 无凝结
MTBF	25 万小时	25 万小时	25 万小时
电源	90-265V AC，冗余供电	100-240V AC，冗余电源	100-240V AC，冗余电源
最高功率	<20W	<48W	<48W
尺寸（宽*深*高）	430x482x44mm	440*400*44mm	440*400*44mm
安装方式	标准机架式安装	标准机架式安装	标准机架式安装

应用场景



过程监控层异常通讯行为检测

- 以旁路方式部署在过程监控层
- 基于智能学习模式，自动建立通信模型基线，对不符合通信模型基线的通信行为进行告警
- 监测过程监控层设备的流入流出流量，并设置基线值，超出基线值将产生告警
- 对工控系统工程师站组态变更、操控指令变更、PLC下装、所有写操作、负载变更等关键事件进行实时监控

现场控制层异常操作指令检测

- 以旁路方式部署在现场控制层
- 监测现场控制层设备流量，当设备出现端口、软件、网络、协议故障导致无流量时，产生告警信息
- 基于工控协议通信记录，智能学习通信关系、功能码和参数，对正常通信行为建模，实现违规行为监测审计
- 详细记录网络中的连接信息，包括开始时间、结束时间、源MAC、目的MAC、报文数（上行、下行）、字节数（上行、下行）、端口号、功能码等