360 网神工业工业安全监测系统

产品白皮书

目 录 | Contents

一. 引言

随着工业信息化的快速发展，工业化与信息化的融合趋势越来越明显，工业控制系统也在利用最新的计算机网络技术来提高系统间的集成、互联以及信息化管理水平。未来为了提高生产效率和效益，工控网络会越来越开放，而开放带来的安全问题将成为制约两化融合以及工业 4.0 发展的重要因素。目前，工业控制系统受到了越来越多的安全威胁，其中既有来自敌对政府、恐怖组织、商业间谍、内部不法人员、外部非法入侵者等的攻击与破坏，也有由于系统复杂性、人为事故、操作失误、设备故障和自然灾害等造成的工业控制系统损害。然而，这些安全威胁往往长期存在于工控系统中，并难以及时发现和预防，给企业的安全管理带来了诸多问题：

- 网络安全管理混乱缺少“抓手”；
- 资产难以管理（设备数量、类型、工作状态不清楚）；
- 工控系统漏洞难以及时发现并修补；
- 工控系统非法操作、通信异常难发现；
- 工控系统遭受网络攻击以及时发现并追根溯源；
- 工控网络病毒传播难以发现并定位处置；

……

工控系统的安全问题可以分为三个方面：资产状况、安全威胁和生产故障。首先，工控系统包含控制器、主机、服务器、网络设备等资产，这些设备存在着数量大、厂商类型多、部署分散、系统老旧、漏洞较多等问题。其次，工控系统容易遭受渗透攻击、僵尸主机、病毒传播等安全威胁。最后，工控系统的生产过程容易发生设备故障、异常操作、非法指令等异常。

图 1.工控系统安全问题分类

目前市场上的检测类产品无法满足当前工控系统安全管理要求。传统的信息安全监测类产品主要针对传统 IT 安全，对工控场景支持不足，如不支持工控协议、无法识别工业资产、无法对工控流量进行精细化审计。而专门的工控审计类产品对 IT 流量威胁支持不足，如不支持网络入侵检测、不支持病毒检测。因此随着 IT 和 OT 网络的融合，工控系统的安全监测需要的是对 IT 和 OT 安全风险进行全方位展示。恐惧源于未知，看见才能安全。只有看见、看清、看透、看全工控系统中的威胁和隐患，才是保障工业安全的基础和前提。

二. 工业安全监测系统产品介绍

2.1 产品概述

360 网神工业安全监测系统（简称 ISD，Industrial Security Detection）是 360 企业安全集团全新推出的工业安全检测类产品。是基于业界领先的软、硬件架构开发的一体化产品，软件层面上，具备完全自主知识产权的鲲鹏网络操作系统，并结合工业特性的协议深度检测引擎（DPI），实现对工控协议的 L2~L7 层全解析，并支持多种主流工控协议。

产品通过接入镜像流量的方式部署，旁路被动的采集方式对工控系统网络不会造成影响。可部署于企业办公网、生产管理层、过程监控层、现场控制层，通过智能学习建模技术，识别系统中存在异常事件。并通过 IDS 和 AV 引擎技术，发现信息安全威胁，对工控系统进行全方位监测和保

护。协助运营人员及时进行响应处理，提升工业生产连续性水平。适用于电力、石油石化、轨交、制造、煤炭、烟草、钢铁等多行业。

2.2 产品架构

工业安全监测系统采用专用架构硬件平台，软硬一体化设计，可以有效降低硬件漏洞，增加安全性，提高稳定性、可靠性。具备完全自主知识产权的鲲鹏网络操作系统，多核 AMP+软件架构，在高安全性、高开放性、高扩展性和高可移植性基础之上，结合工业特性的协议深度解析引擎重点加强了防御能力、数据生成能力、数据分析能力、数据处置能力，让工业安全监测系统具备深度解析、智能学习、异常处理、风险信息全方位展示分析及审计的能力，并能提供多维度的有效信息帮助用户完成日常维护工作。

同时，工业安全监测系统集设备工控协议解析、工业异常发现、网络威胁发现、审计于一体，极大提高了底层硬件的安全性、工控协议解析处理速度。

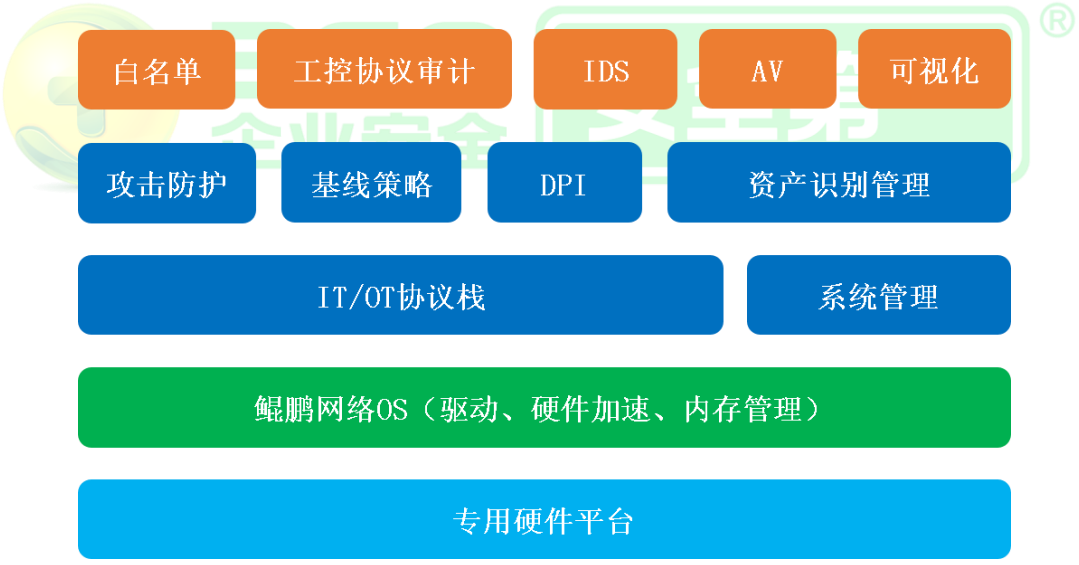

图 2. 工业安全监测系统架构图

2.3 产品功能

2.3.1 资产发现和管理

工业安全监测系统通过旁路无损流量探测技术，可自动发现并识别工控设备类型。支持多种设

备类型包括 PLC、DCS、HMI、RTU，支持多个主流厂商品牌包括西门子、施耐德、罗克韦尔。通过自动学习建立工控通信模型，形成资产白名单，监测非法设备接入。对已经发现的资产进行管理，发现资产的脆弱性隐患，包括资产所对应的漏洞信息、开放端口脆弱性和使用的不安全的协议。

2.3.2 精准的应用识别

工业安全监测系统搭载 360 企业安全自研的深度数据包解析引擎，可对网络流量做到实时解析和精准的识别，并将每条网络通信连接以流量日志的形式存储。支持 2000 种以上的应用识别，包括传统 IT 网络协议、多媒体软件、办公软件、通讯工具、流媒体等，同时也全面支持主流的工控协议。

2.3.3 指令级白名单检测

工业安全监测系统基于深度数据包解析引擎，全面支持各大主流工业控制协议，并且能够对各类数据包进行快速有针对性的捕获与深度解析。对不同行业的工控系统，可以采取相应针对性的数据包解析策略，能够检测出数据包的有效指令、数据内容和负载信息，并结合白名单对不符合规则的流量进行告警。深度数据包解析引擎涵盖 OPC、Modbus、IEC104、S7、MMS、DNP3、EIP、FINS 等主流工控协议。支持预定义模版，可以对 OPC、Modbus、S7 协议进行只读设置。

2.3.4 运行异常监测

工业安全监测系统通过深度数据包解析引擎，对生产工艺中的关键事件进行检测，如：工程师站组态变更、操控指令变更、PLC 下装、固件升级等关键事件。通过网络基线模块监测偏离基线的异常操作，告警设备违规外联以及人员违规操作。

2.3.5 学习模式

工业安全监测系统支持两种工作模式，学习模式和告警模式。学习模式应用于工控网络信息安全规划阶段，安全管理人员不了解工控网络情况，可以通过学习模式对工控网络中的协议和流量行为进行被动式的学习，从而自动生成相关策略，学习模式下的网络流量行为不会产生告警。告警模

式应用于工控系统安全运行阶段，安全管理人员根据学习到的规制以及实际需要对工业安全监测系统进行策略配置，策略正式生，在告警模式下不符合安全策略的数据流会产生告警日志。支持学习模式的功能包括资产识别、网络基线和工控协议白名单。

2.3.6 威胁检测

工业安全监测系统通过内置的 IDS 入侵检测引擎和 AV 反病毒引擎，实时检测工控系网络中的威胁行为。IDS 引擎支持缓冲区溢出、跨站脚本、拒绝服务、恶意扫描、SQL 注入、WEB 攻击。AV 引擎支持对传统 IT 协议中传输的文本、附件内容进行解析提取。对提取后的数据进行病毒扫描，支持的协议包括 HTTP、FTP、SMTP、POP3、IMAP、SMB。

2.3.7 攻击检测

工业安全监测系统的网络攻击检测模块通过 Flood 检测、扫描检测、异常包攻击检测、应用层攻击检测等防护手段，将包括 SYN Flood、ICMP Flood、UDP Food、IP Food、 ping of death、Teardrop、IP 选项、TCP 异常、Smurf、Fraggle、Land、Winnuke 等常见的攻击行为检测集成在模块中。用户可通过启用对用防护模块，可以有效的检测非正常报文流入工控网络，对工控协议内网服务进行保护。

2.3.8 全方位可视化

工业安全监测系统为用户提供了仪表板和大屏展示，全面的实时的可视化信息展示，着重突出资产信息、应用协议信息、流量信息和威胁事件，可以对威胁、应用、会话、网络的全方位监控与分析、日志审计，确认异常行为是否具有风险。

2.4 产品优势

2.4.1 以资产为中心威胁分析，符合客户习惯

工业生产流程比较固定，相较于以告警事件为中心的威胁分析方案，以资产为中心的漏洞发现

与风险分析更符合工业环境管理习惯。

2.4.2 级联无损部署方式，不影响生产

产品支持部署在不同层级（集团，厂区，车间），通过控制平台统一日志分析与策略管理，满足客户分级监管需求。此外，旁路工作模式不影响现有工业生产。

2.4.3 全面检测 IT/OT 安全威胁

集 AV 检测、IDS 检测、白名单监测、工控关键操作监测引擎于一体，全面检测工业网络的病毒传播、入侵行为。兼备传统 IT 网络与工控网络安全检测能力，适合 IT/OT 混合网络环境。

2.4.4 安全威胁多维视角大屏呈现

从资产、脆弱性、威胁等多个视角全面分析工控系统安全态势。采用业内最先进的大屏可视化技术，直观呈现工控系统安全态势。

2.4.5 工控协议深度解析

精准的工控协议指令级解析，对工控协议做到实时和精准的识别，支持 OPC、Modbus、IEC104、S7、IEC61850、DNP3、EIP、FINS 等主流工控协议。在遵循工业控制系统可用性与完整性的基础上，能够检测出数据包的有效内容特征、负载和可用匹配信息，如恶意软件、具体数据和应用程序类型。

2.5 典型部署

根据工控系统的标准普渡分层模型（由上至下，企业 IT 层、生产管理层、过程监控层、现场控制层、现场设备层），ISD 作为旁路设备，可以部署在 L1~L3 层的位置，通过监测对应网络交换机的镜像端口流量，实现对该区域网络的监测审计，如图：

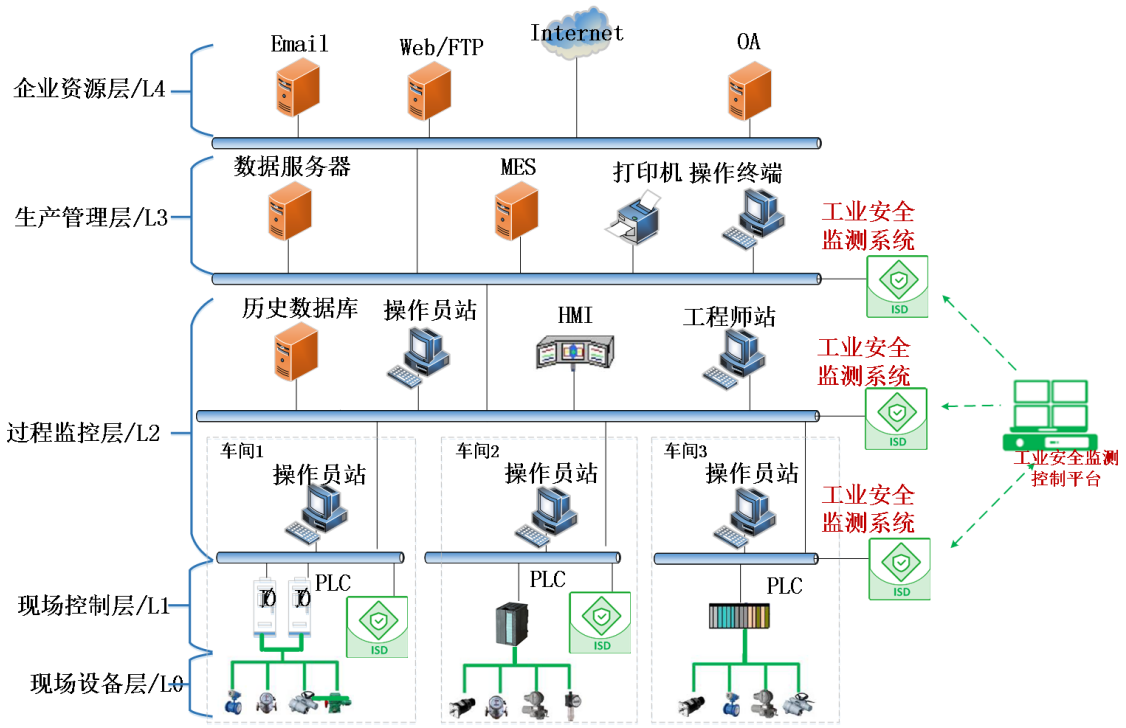

图 3. 工业安全监测系统部署

“多点分布集中上报”，对于拓扑相对复杂的工控系统来说，需要根据生产业务、地理位置不同因素，通过使用多个接入工业交换机的方式，将网络划分成多个区域，如图。针对这样的网络，我们需要将 ISD 部署到每一个接入交换机一侧，才能实现对每一个子网内流量的监测，同时也许要将 ISD 部署在汇聚（核心）交换机一侧，以实现对 OT 到 IT 之间的流量的监测。ISD 需要将采集到的数据信息，集中上报给 ISDC，以供 ISDC 进行流量分析和问题处置。

三. 客户价值

3.1.1 为企业提供了工控系统安全管理的抓手

工控网络（OT）由于在工作要求和设计目标上与 IT 网络存在显著差异，IT 网络的安全防护手段不能直接应用到 OT，导致 OT 安全管理缺乏方法和工具。360 工业安全检测系统为 OT 管理提供了有效抓手。

3.1.2 监测网络攻击与异常操作，降低事故风险

系统内置 IDS（入侵检测）引擎和 AV 检测引擎，实时检测攻击流量，及时对危害生产安全的网络攻击发出报警。系统实时监测生产过程中的关键事件，如：组态变更、操控指令变更等操作。对于偏离基线的行为及时告警，以避免由于设备违规外联、人员违规操作导致的停产风险。

3.1.3 帮助企业进行安全预防性维护、应急响应和事故的调查

工业安全监测系统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，提供了简便易用的回溯功能，为工控系统的安全事故调查提供了坚实的数据支持，改变以往工业控制系统出了安全事故无法取证、调查无从下手的被动局面。

3.1.4 满足政策合规要求，降低安全责任风险

通过对工控系统的安全审计监测，满足等保和行业安全的基本合规要求，并可对日志进行回溯查询，从而降低安全责任风险。