案例

公司名称：奇安信科技集团股份有限公司

主标题：石油天然气管道工控系统安全监测与态势感知

副标题：保障国家关键基础设施安全

引言：

奇安信科技集团股份有限公司（以下简称“奇安信”）是中国最大的网络安全公司之一，专门为政府、军队、企业，教育、金融等机构和组织提供企业级网络安全技术、产品和服务，已覆盖 90%以上的中央政府部门、中央企业和大型银行，已在印度尼西亚、新加坡、加拿大、中国香港等国家和地区开展了安全业务。

奇安信工业互联网安全事业部基于自身在大数据、威胁情报、防病毒、安全攻防、态势感知等方面的突出优势，创新性的提出了“数据驱动工业安全”的技术发展理念，构建了层次清晰、定位明确、融合联动的工业信息安全产品体系。

石油天然气管道承担国家战略物资的传输任务，其工控系统属于国家关键基础设施。奇安信通过本项目的实施，帮助客户对管道工控系统整体安全态势进行监测和响应处置，提升了其安全与可靠性运营水平。

一、项目概况

1. 项目背景

近年来石油天然气基础设施已经成为黑客组织的攻击目标，2017 年发生的

针对沙特某石油天然气装置功能安全仪表系统（SIS）的攻击为各国网络安全主管机构和基础设施运营企业敲响了警钟。

本项目用户负责长距离输油气管道的运营管理、建设和科研，承载着国家重大战略物资输送的任务，拥有集油气管道输送技术研发、服务、培训、检测和监测为一体的专业科研机构，科研力量雄厚，科研设施完备，拥有管道核心技术研发能力，在油气储运工艺、管道完整性管理、管道化学添加剂、管道规划、信息与经济等研究领域整体处于国内领先水平。

2. 项目简介

本项目实现对客户辖区内工业网络全方位、全天候的安全监测，对工控系统的资产进行实时发现和监测，帮助用户实现工控系统的“可视化”，及时发现各类网络安全风险以及非法访问事件，实现工业信息安全的闭环管理，全面提高管道公司工业安全防护的整体水平。

3. 项目目标

用户承担着国家重大战略物资输送的任务，其油气调控系统属于国家关键信息基础设施，一旦遭受攻击，损失极大。为贯彻、落实习总书记 4.19 讲话精神，按照《网络安全法》及相关标准要求，本项目建设油气调控系统分控中心工控系统安全监测与态势感知平台，协助运营人员及时进行处置响应，提升油气传输可靠性。

二、项目实施概况

通过前期调研了解到，各厂站端的工业流量汇聚到分控中心。为能够实时采集流量、不影响现有工业网络，采取了在交换机旁路部署工业安全监测系统（ISD）进行安全监测，在分控中心采用工业安全监测控制平台（ISDC）进行整体态势感知的解决方案。

1. 项目总体架构和主要内容

根据普渡模型，ISD 和 ISDC 总体部署模式如下图所示：

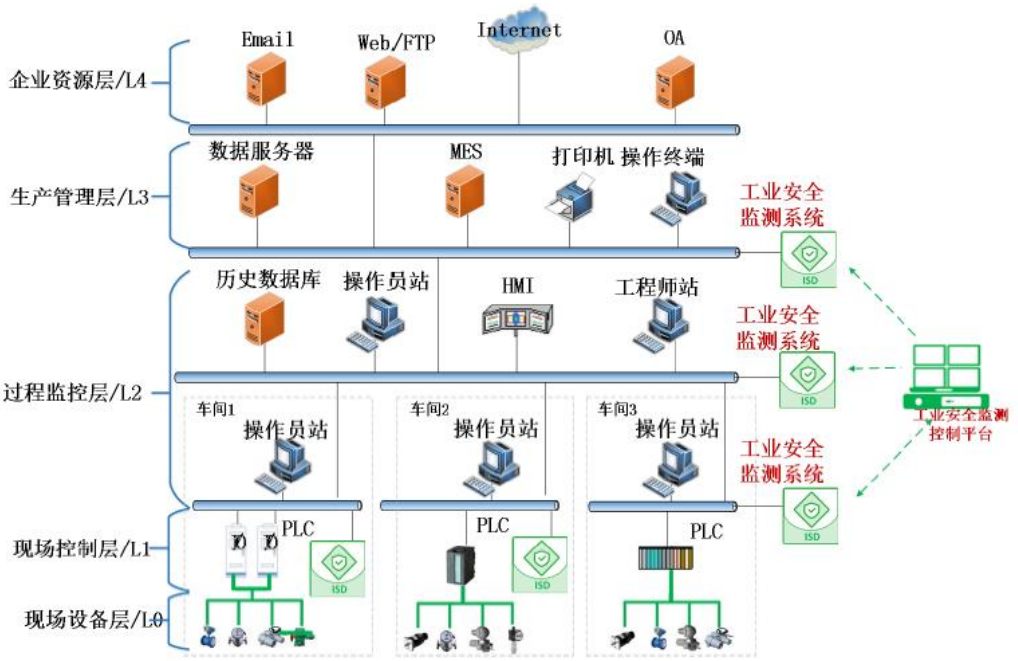

图 1　基于普渡模型的产品部署模式

工业安全监测系统（ISD）是针对工控系统网络环境进行异常监测、威胁发现和安全审计的一体化产品。产品通过旁路方式部署，对工控系统的运行数据进行被动无损采集，实时发现信息安全威胁和其造成的系统运行异常。产品可部署于生产管理层、过程监控层、现场控制层，协助运营人员及时发现问题并响应处理，提升工业生产连续性水平。

工业安全监测控制平台（ISDC）采集分布式部署在工业控制系统中的工业安全监测系统（ISD）、工业主机防护，工控防火墙相关数据，以可视化方式集中展示资产、拓扑、威胁、脆弱性和工控系统安全运行状况，对安全事件进行场景化分析、集中管理和处置跟踪。

2. 网络、平台或安全互联架构

本项目工控系统安全监测与态势感知平台部署示意如下图所示，工业安全监测系统（ISD）采用交换机旁路部署模式，工业安全监测控制平台对系统安全进行整体安全监测与态势感知。

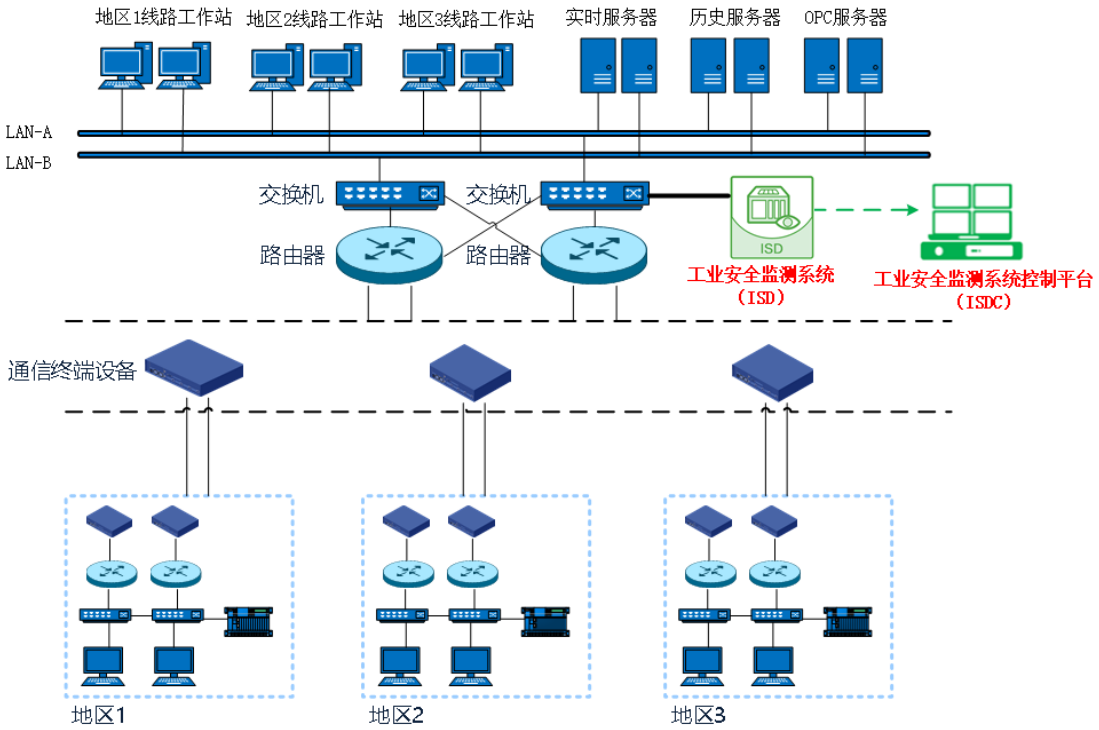

图 2　现场工业安全监测部署示意图

3. 具体应用场景和应用模式

本项目在油气调控行业背景下实现以下安全功能：

（1）自动资产发现

基于被动流量发现资产，支持多种厂商型号控制器，包括西门子，施耐德，罗克韦尔等。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。支持资产管理，可管理厂商名称、设备类型、设备型号、IP地址、MAC地址、使用协议、重要性等。

（2）无损漏洞识别

对识别后的资产进行脆弱性检查，包括资产所对应的漏洞信息、开放的端口和不安全的协议。其中漏洞识别支持3大漏洞库CVE，CNVD，CNNVD，覆盖220+厂商，3300+条漏洞。由于是被动的流量识别，相对于主动漏洞扫描的方式安全无损。

（3）网络威胁检测

系统内嵌IDS入侵检测引擎和AV反病毒引擎，实时检测工控系统网络中的威胁行为。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攻击等。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等。

同时内置攻击检测模块，支持对Flood攻击、扫描、畸形包攻击、应用层攻击的实时检测。用户通过启用对应防护模块，有效的检测工控网络中非正常报文，提升防护能力。

（4）异常操作监测

通过搭载的数据包解析引擎对关键事件进行检测，如：工程师站组态变更、操控指令变更、PLC下装、固件升级等。本功能同时支持对OPC、Modbus TCP、S7、IEC104、CIP协议的白名单检测，可以针对各类数据包进行快速有针对性的捕获与深度解析，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。

（5）系统状态监测

进行流量审计，实时监测工控系统网络通信情况。可识别多种主流工业控制协议，支持2000+种IT常用应用协议识别，可识别工控系统内的违规IT应用，例如游戏、视频、社交应用。基于网络基线模块监测偏离基线的异常流量，识别设备断线、非法连接等异常。

（6）响应工单处置

在发现高危告警后，安全管理员可将告警内容和响应建议通过工单方式发送给指定的安全事件处置人员,对告警的处理进行闭环管理、统计和分析。

（7）自动报表生成

提供灵活的报表管理功能，可以支持快速报表，实时的输出期望的报表内容，也可按照客户指定的周期自动生成报表以帮助用户周期回顾安全情况。同时系统提供了报表模板的灵活编辑，用户可以根据自身需要在数十个预置报表展示内容中选择自身需要内容，调整顺序以形成自身需要的报表。对于用户定制化的报表内容，安全团队可以根据情况进行报表定制以应对中国式报表需要。

（8）动态大屏展示

为用户提供了大屏展示模块和仪表盘功能，提供全面实时的信息展示。从资

产、协议流量、网络威胁等多个视角，结合实时曲线、动态占比、动态排行等显示模块，对工控系统网络安全状况进行直观展示。

4. 方案特点

（1）以资产为中心

产品通过资产自动识别、资产管理、资产网络关系图绘制，提供了以资产为中心的安全管理视角。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。级联无损部署方式，不影响生产。

（2）多功能合一

ISD 集流量审计、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。同时满足合规要求和安全监测的要求。

（3）直观的可视化效果

工业安全监测控制平台 ISDC 利用可视化技术，将收集的数据进行直观的可视化展现，包括 2D/3D 地图，条形统计图等各种形式，通过对数据的直观展示，用户可以清晰的了解到当前网络安全态势。

三、项目创新点和实施效果

1. 项目先进性及创新点

（1）以“大数据分析”为核心的威胁发现和溯源技术

大数据时代的到来为工业信息安全提供了新的技术手段，对工业企业的业务数据和安全数据进行统一管理，将工业大数据和信息安全分析技术相结合，实现对数据的采集、分析并从功能维度进行汇总、查看、统计及处置。基于大数据处理的工业态势感知成为对工控系统安全威胁和系统状态异常分析的有力武器。利用大数据分析能够对安全态势、攻击源、攻击事件和工控资产进行可

视化展示，并通过可视化界面进行数据关联查询，及时对工控环境中未来风险进行预测、预防。最终做到“四得”：看得清用户、抓得住行为、报得准风险和响应得及时。

（2）以“积极防御”为核心的纵深防御技术

为了实现持续的安全风险管理目标，企业需要建立能够随着时间不断演进的安全架构和技术支撑体系。本平台基于网络安全滑动标尺模型进行安全防护。该标尺模型共包含五大类别，分别为架构安全、被动防御、积极防御、情报和进攻。这五大类别之间具有连续性关系，并有效展示了防御逐步提升的理念，形成纵深防护体系。

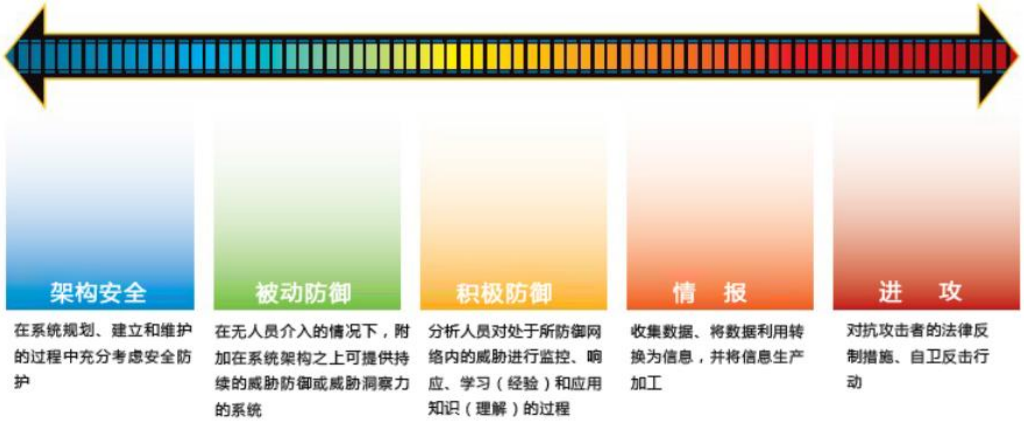

图 3　网络安全滑动标尺模型

架构安全：在系统规划、建立和维护的过程中充分考虑安全防护。

被动防御：在无人员介入的情况下，附加在系统架构之上可提供持续的威胁防御或威胁洞察力的系统。

积极防御： 分析人员对处于所防御网络内的威胁进行监控、响应、学习（经验）和应用知识（理解）的过程。

情报：收集数据、将数据利用转换为信息，并将信息生产加工为评估结果以填补已知知识缺口的过程。

进攻：在友好网络之外对攻击者采取的直接行动（按照国内网络安全法要求，对于企业来说主要是通过法律手段对攻击者进行反击）。

现阶段大多数企业的信息安全工作都聚焦于“架构安全”和“被动防御”对“积极防御”和“情报”则涉及较少，本项目建设以 “情报”驱动的“积极防御”纵深防御平台，提高企业的网络安全防护能力。

（3）以“人+机器”为核心的安全运营技术

新形势下的网络安全，本质是“三人”的对抗：人与人的对抗、人与机器的对抗、人工智能的对抗。人工智能时代，机器人可以替代一切，但不能替代网络安全工程师，因为网络安全是逆向思维、是不走寻常路，而人工智能是经验的决定。只有采用“人+机器”的方法，把人的知识驱动和机器的数据驱动结合起来，才能真正做到“谁进来？做什么？拿了什么？”，从而掌控全局。

2. 实施效果

本项目采用奇安信工业安全监测系统（ISD）和工业安全监测控制平台（ISDC）对油气调控系统进行集中监测，该项目为中石油管道系统首套大型工控系统安全监测与态势感知平台应用，提升了油气传输可靠性，降低安全运营成本，为下一步在中石油及其它大型工业企业推进奇安信倡导的工业安全监测和响应体系建设奠定基础。