1.1 案例四：钢铁行业工控安全纵深防御解决方案——基于IT和OT融合技术构建钢铁行业网络安全防御体系

1.1.1 方案概述

本方案针对现有信息系统的安全管理中心、计算环境安全、区域边界安全和通信网络安全进行合规的总体框架设计。建立以计算环境安全为基础，以区域边界安全、通信网络安全为保障，以安全管理中心为核心的信息安全整体保障框架体系，并通过安全监测预警、安全主动防御、及时安全响应、有效安全恢复的技术手段，将信息系统构建成具备主动防御、多级防护、纵深防控、整体保护能力的安全、可靠信息系统。

1.方案背景

钢铁企业主要生产工艺流程有：焦化、炼铁、炼焦制气、炼钢、钢轧、冷轧薄、动力等；每个工业流程均是由以PLC+工业PC+工业通讯网络构成的自动化控制系统。PLC系统由PLC控制柜、通讯柜、端子柜组成。现场来的电缆先接入端子柜,再由端子柜接至PLC，PLC与上位机通过工业交换机进行数据交换。不同PLC系统与其它PLC系统有关的连锁信号通过网络通讯完成数据交换。钢铁厂工业以太网一般采用环网结构，为实时控制网，负责控制器、操作站和工程师站之间过程控制数据实时通讯，网络上所有操作站、数采机和PLC都采用以太网接口，网络中远距离传输介质为光缆，本地传输介质为网线（如PLC与操作站之间）。生产监控主机利用双网卡结构与管理网互联。钢铁企业的工业控制系统具有多个生产工艺流程混合、控制网络组网复杂，多种通信方式并存、生产控制系统品牌多、新老系统并存，多种高级应用分而自治，使得可以被黑客利用的漏洞大量存在。可见，

对于这样的系统网络，不能采用单一的防护策略，需要根据实际情况，从不同角度和层次应用多种策略进行综合防护。

随着工业互联网和钢铁行业信息化的推进以及 MES、EMS、APS 等系统的逐步推广应用，原本相互独立的 DCS、PLC、电仪系统、SCADA 等控制子系统需要通过网络与信息系统连接在一起。这些控制子系统负责完成对高炉控制系统、转炉控制系统、燃烧控制系统、炼钢智能控制系统、轧薄带智能控制系统、高精度板厚控制系统的采集、存储、输送等控制任务，一旦受到恶性攻击、病毒感染，就会导致钢铁生产受到严重影响，甚至造成人员伤亡等严重后果。在钢铁行业统一管理集中监控的大趋势下，工业控制系统网络的集成度越来越高，与其他信息网络的互联程度也随之提高。与此同时，未经隔离的网络与主机、误操作、恶意操作、未授权的接入与操作、未授权的程序安装、系统资源滥用与误用、外部接口滥用（usb 口及其他扩展接口）以及新型攻击（APT）也对工业控制系统安全带来极大的威胁。如果工业控制系统不加强主动防护、监测审计、集中监管和预警响应等安全措施的建设，将在系统中留下大量的安全盲点与灰色地带，给各类外部威胁留下可乘之机，不但无法对安全事件做到及时响应处置，还非常容易对生产业务产生严重的影响。

2.方案简介

目前钢铁企业工控系统各个系统之间互联互通密切，随着网络化的逐渐深入，新的场景也带来了新的风险，钢铁企业目前面临不同的生产区域之间为了连接的便利性未做有效的区域划分、工业控制通信协议在设计时通常只强调通信的实时性及可用性对安全性普遍考虑不足、工控上位机大多数处于“裸奔”状态、软件开发阶段缺少安全设计软件存在大量的安全漏洞、员工安全意识淡薄等等一系列安全问

题。

依据《网络安全法》、“等保 2.0”等现行法规、规范和标准的要求，在安全分区、网络专用、横向隔离、纵向加密、分级综合防护的基础上，通过工控网络“智能白名单”形式，对钢铁厂生产控制大区系统进行自主可控、安全可靠的工控安全整体防护。利用“AI 基因，威胁免疫”安全防护技术构建钢铁厂网络信息安全综合防护架构；完善钢铁厂生产控制大区工控网络信息安全防护体系，符合工控等保 2.0 第三级安全防护要求。

3.方案目标

建立自动化生产系统的安全加固与主动预警的安全防护体系，从网络层、主机层、系统层、应用层和管理制度等多方面进行主动式威胁管理，提高工业控制系统整体安全防护等级，保证钢铁企业工业控制系统的稳定有序运行。

（1）建设工控网络边界安全防护及终端计算环境安全防护

通过技术手段对在工控网络边界部署安全产品，以钢铁生产工艺流程为单位，对安全生产网络进行安全域的划分，坚持“横向分区、纵向分层”的原则构建可信工控系统，防护网络攻击与威胁，保证工业生产系统安全，打造工控安全计算白环境；部署统一运维平台进行工控网络安全工作高效可靠管理，初步建立工控网络安全管理体系，即利用技术手段和管理手段保证企业安全生产。

（2）建设完善的安全审计措施和未知威胁检测，完善纵深防御体系

通过旁路监听与智能分析技术，对系统的控制、采集请求、网络行为进行详细的审计，对攻击及时预警。建立事前攻击的提前发现和预防，事中攻击的主动检测、主动防御，事后及时溯源，做到应急响

应。同时构建清晰的资产互访拓扑；对攻击场景进行还原，对每个攻击阶段进行回溯分析，通过丰富的可视化技术进行多维呈现。

（3）建设网络安全监测预警与信息通报平台

建立针对钢铁行业各工艺段工业互联网安全监测预警、信息通报、应急处置手段，提高威胁信息的共享，对监测发现的安全风险隐患及时通报相关企业；实现工业设备资产感知、工业漏洞感知、工业配置感知、工业协议识别和分析、工业连接和网络行为感知、工业僵木蠕检测、工业攻击链的监测和分析等安全态感知功能，实时识别和预警工业控制网络和工业互联网络的安全威胁，及时与工业安全设备联动实现协同防护，并提供攻击回溯取证和安全态势定期报表，为制定工控安全策略提供支撑，形成安全闭环，进而实现工业控制网络和工业互联网络安全威胁的可视、可控、可管。

1.1.2 方案实施概况

鉴于当前钢铁行业工控系统安全现状，若要同层级不同区域的纵深防护，需要对工业网络内部通信的各种数据采集协议和控制协议进行深度解析，对工控网络进行区域划分与隔离，对工控主机进行安全加固，对工控网络进行全网安全审计和威胁感知。

1. 方案总体架构和主要内容

（1）方案总体架构

工控系统安全建设遵循“一个中心，三重防护”的建设原则，在钢铁厂集团数据中心建设工控安全管理平台、工控安全态势平台及工控系统数据灾备中心。

该厂均在内部建设独立的工控安全管理平台和工控安全态势感知平台，本部生产基地为数据分析中心，各基地平台将数据上传至本部生产基地工控安全管理平台和工控安全态势感知平台进行审计分

析、数据综合分析与展示。

数据灾备中心将各厂区重要业务系统的数据集中汇总收集，集中灾备，避免意外造成的数据丢失。

在集团下各分厂搭建纵深的三重防护体系，以安全服务的形式梳理通信网络，理清网络边界，在网络边界构建访问控制体系，阻断非正常的边界访问，搭建分支管理中心，对计算环境进行综合监管与安全审计，对终端设备进行安全运维，对终端系统进行白名单准入管控。

拓扑架构如图 4-1 所示：

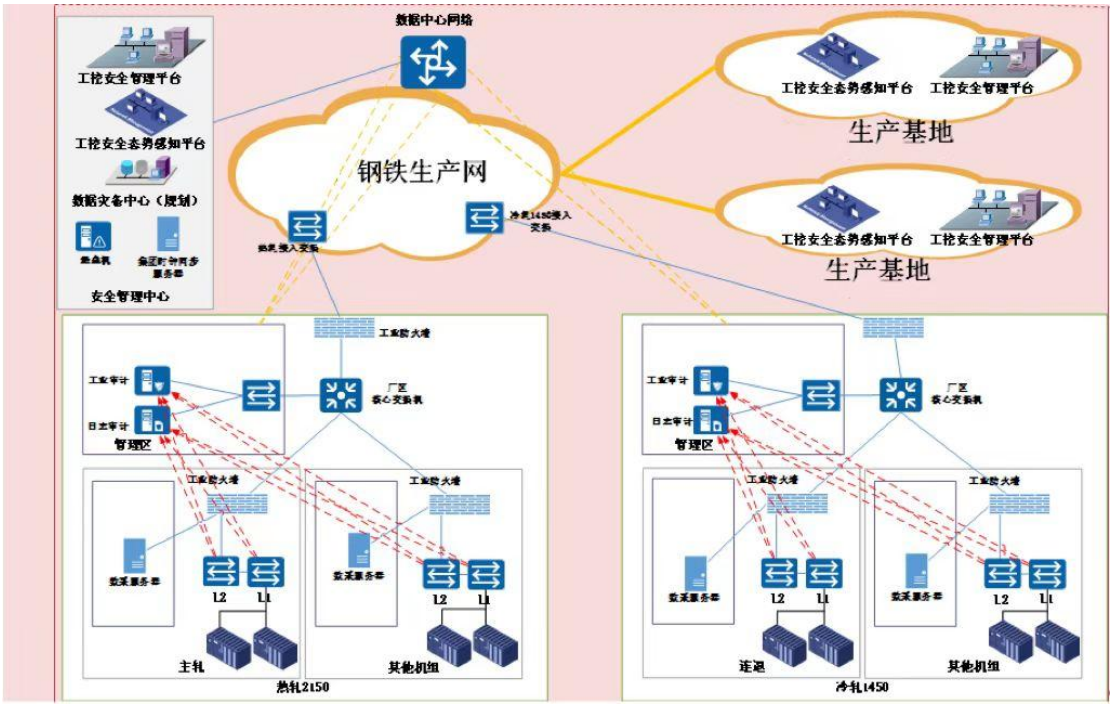

图 4-1　拓扑架构

在部署防护措施的时候，首先做好网络隔离安全，明确网络边界，基于数字证书等措施进行身份认证和授权管理，基于零信任措施严格执行细粒度的访问控制；

其次在生产控制网部署工业监测审计设备记录应用和设备情况，学习通信和数据的特点，结合主机白名单软件建立工控网络安全“白环境”。

再次采用堡垒机应对工控网络系统管理员特权以及非法操作等突出安全问题；

然后采取综合审计措施，对网络安全事件进行发现和追溯管理；

最后基于安全服务，对生产厂全网进行安全加固，逐一终端检查本地安全服务及本地安全策略，排查弱口令，雷同口令，非法外设等，并利用备份机制和并行机制，结合应急响应预案建立快速响应能力。

（2）方案主要内容

- **安全域划分**

厂内各机组按分厂（分线）统一安全监控。按具体情况：

其一，L2 网络能够连接成一个网络的情况，可以在 L2 机房（或主电室）配置核心交换机统一与生产网汇聚交换机连通，分期分阶段将网络汇聚到厂内 L2 机房（或主电室）核心交换机。各机组网络用工业防火墙进行隔离，可以根据需要进行连通（或不连通）；

其二，L2 系统无法进行统一接入的情况，L2 通讯服务器就近接入到生产网的接入交换机，中间用工业防火墙进行隔离。

内部安全域划分上，首先，基于三层交换机，按 IP 地址为生产网划分 VLAN，并设置子网地址。采用 VLAN 提供的安全机制，可以限制特定用户的访问，甚至锁定网络成员的 MAC 地址，这样，就限制了未经安全许可的用户和网络成员对网络的使用。如无法划分 VLAN，可以在工业防火墙启用 NAT 功能；其次，配置交换机的（ACL）访问控制策略，通过包过滤技术禁止外部非法用户对内部的访问。同时建议关闭或限制使用交换机、路由器等网络设备的不必要功能、端口、协议和服务。

管理网与工控网边界：在管理网与工控网之间均采用工业网闸进行网络隔离。能够阻止不必要的流量进入工控网。仅定义必要的工控

应用服务器与管理网的业务服务器允许通信，其他通信都被禁止。最大限度的阻止从管理网络向工控网络入侵行为的传播，同时保证必要的业务系统间的数据共享。满足等保 2.0“安全网络通信”中：保证跨越边界的访问和数据流通过边界防护设备提供的受控接口进行通信的合规要求。

各生产子网的边界：在网络之间采用工业防火墙进行隔离。阻止生产子网以外的数据包或恶意程序进入生产子网，限制子网内的允许跨网通信的主机数量，除非必要，否则将禁止子网间的通信。同时防止一个子网感染病毒后向其他子网或上层安全域传播的可能。工业防火墙具有工控网络通信协议的深度内容检查功能，能够及时发现功能码错误或指令攻击行为，提供阻断或报警功能。

安全管理中心边界：安全管理中心因为必须在网络上与被管理设备间路由可达，防火墙应设置端到端的、基于端口的严格访问控制规则，阻止对安全管理中心的非授权访问行为，阻止来自任意网络对安全管理域的不必要流量，保障管理中心自身安全。

未知边界管理：由于工控网络的物理边界范围太大，给管理带来非常大的难度，随身 WIFI 设备、无线路由私接、手机热点等都随时可能破坏网络边界的完整性，使得用户在网络边界上的努力和投入化为乌有。在网络核心处部署边界完整性检查产品，快速网络检测、定位与阻断控制破坏网络边界行为，保护边界安全。

- **纵深安全防御**

基于边界访问控制、边界入侵防御等构建纵深安全防御体系。入侵防御是工业控制系统安全防护的重要技术措施。在工业防火墙选择工业入侵防御模块，可以实时监控关键业务系统的关键路径信息，实现安全事件的可发现、可追踪、可审计和阻断。

工业入侵防御系统采用协议分析、模式匹配、异常检测等技术，实现对网络流量、数据包的动态监视、记录和管理、对异常事件进行告警等。满足等保2.0“安全网络通信”中：在关键网络节点处检测、防止或限制从外部（或内部）发起的网络攻击行为的合规要求。

- **网络安全预警**

通过在网络关键节点处对数据流量做镜像采集，并交由中心节点的分析平台做数据分析的方式进行安全分析与威胁预警。采用“AI基因，威胁免疫”的防护理念，运用人工智能技术实现对安全威胁的主动防御，能够在攻击产生破坏行为之前及时被发现并响应，避免发生更大的经济损失与社会影响。

通过新一代高性能分布式大数据平台，搭载大数据AI分析引擎，采用无监督学习算法，以产线内资产为核心构建AI模型，全面检测高级威胁和未知威胁。

通过聚焦于资产发现和未知威胁检测两大客户痛点，通过高效处理海量数据，自动发现内网资产，构建清晰的资产互访拓扑；通过全流量AI未知威胁检测，结合全球威胁情报进行威胁溯源；通过精准攻击场景还原，采用攻击链对每个攻击阶段进行回溯分析，并留存攻击取证报文；结合AI检测、规则检测进行关联分析，自动评估风险资产，通过丰富的可视化技术进行多维呈现。

2. 网络、平台或安全互联架构

（1）网络互联架构

钢铁行业是我国基础性产业，是国民经济的支柱产业之一。相当长的一段时间钢铁企业的工业控制系统一直处于“信息孤岛”状态。近年来，随着互联网+、物联网和智能制造技术的发展，钢铁行业积极推进信息化建设，显著提升了钢铁行业的生产能力和管理水平。钢

铁行业工控系统不断优化升级，这一发展过程中，工业控制系统的网络安全面临着重大挑战。在全球信息化飞速发展的新形势下，如何确保钢铁行业工控系统的信息安全，一直备受重视。

钢铁冶炼是将铁矿石经过一些列工序冶炼成钢并轧制成钢材的过程。为了支撑这一过程，钢厂的工业生产流程还包括了石灰白灰制造，发电，煤的焦化提纯，空气压缩，制氧等一系列能源、辅料以及高价值副产品的生产，工业流程主体如图 4-2 所示：

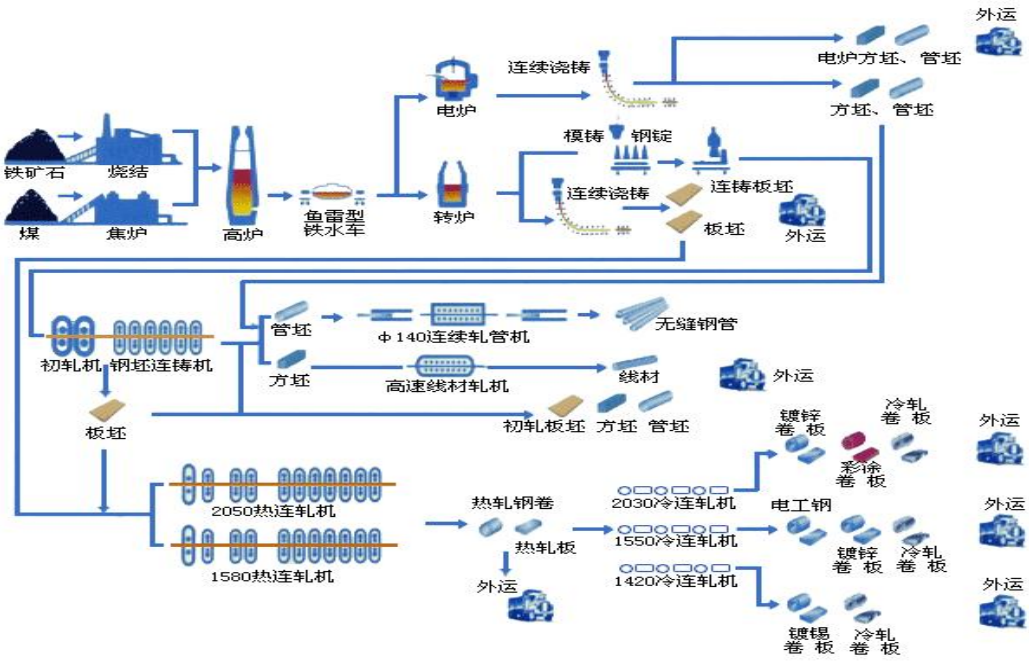

图 4-2　工业流程主体

（2）安全风险

- 生产控制大区内部工控系统边界缺乏有效的防护手段

各生产线之间的网络边界未部署针对工业环境的安全产品，某个域中感染病毒或者受到攻击后，威胁有可能蔓延到整个工控网络。

- 生产监控工业主机及服务器中存在安全隐患

工业控制系统中的主机、工控机未安装专门的工控防护软件，工业主机使用了相对主流的 windows 操作系统，为了保证系统的稳定性

和兼容性往往难以进行必要的安全性补丁更新，在当前的工控网络架构下，其暴露程度也相对较高，存在被植入病毒和各类间谍软件的风险。

根据对工控系统存在的安全风险，得出工控安全建设需求，要以满足未来的等级保护 2.0 工业控制系统安全扩展要求为前提，通过建立多层次的纵深安全防护机制，防止攻击对工控系统造成不良影响，具体建设需求如下：

网络攻击防护：根据该钢铁厂的环网特点，采用适当的网络攻击预警、发现及防护机制，防止网络入侵，恶意软件扩散等情况的出现。

主机安全防护：针对工业主机的特点，采用适当的方案防止恶意软件在工业主机上启动运行。

- 生产控制系统网络内部缺乏完整性管控手段和运维审计措施

在日常的生产运营和维护中，需要第三方运维单位进行设备巡检和检修，为了工作的便捷性，经常将办公用的笔记本及便携设备等接入到生产网络中，由于缺少网络准入技术及安全审计技术，不能对私自接入的设备进行管控，给生产系统带来了很大的安全隐患。在疫情影响下，运维人员还有可能通过远程桌面方式进行运维，缺乏完善的运维审计机制，对运维人员的操作过程没有记录。

3. 具体应用场景和安全应用模式

（1）钢铁行业云数据中心安全防护建设

随着互联网的重心逐步向移动互联网转移，各种新技术新业务上线运营，带来海量数据的爆炸式增长，关于客户的隐私数据也日益增加。因此，需要构建整体全面的云计算安全体系，对内实现安全管理，对外实现安全运营。

在虚拟机资源池环境中，物理服务器内部存在多个虚拟机，每个虚拟机都承载不同业务系统；同时，同一物理服务器内部的不同虚拟机间的流量可以通过内部的虚拟网络层直接通信，不再通过外部的物理防火墙，使得原有的物理安全边界在虚拟化环境下发生改变，因此，原有的安全防护机制无法有效应对虚拟化环境的场景，给云数据中心用户业务上云带来了极大的阻碍。该场景拓扑示意图如图 4-3：

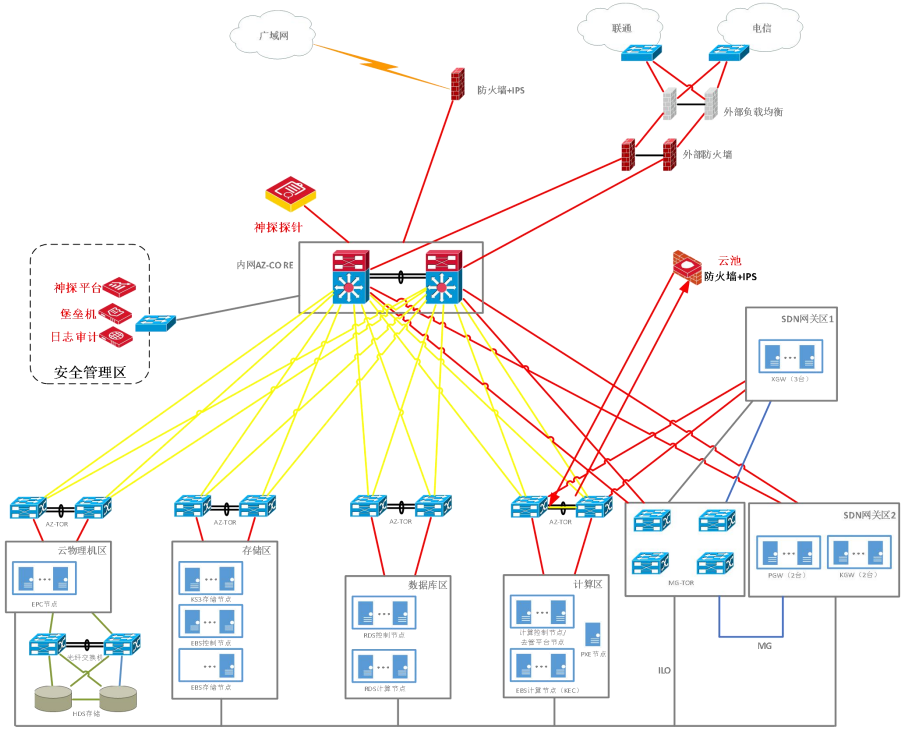

图 4-3　场景拓扑示意图

根据等级保护“一个中心，三重防护”的指导思想，参照《信息安全技术 网络安全等级保护基本要求》第三级安全要求中“安全通用要求”与“云计算安全扩展要求”，通过技术手段实现的防护主要包含如下几个层面：

- 安全通信网络：通过部署六方云池实现租户间的隔离。通过部署云池

产品实现不同云租户虚拟网络间的隔离及边界防护与入侵防范，满足等保中安全通信网络的要求；由于云数据中心网络中有一个不可

控区域，即用户托管的服务器区。此区域的服务器，最终用户拥有完全控制权限，因此此部分很容易被当成肉鸡，直接绕过边界防火墙访问云服务器。因此通过在托管服务器区边界部署下一代防火墙，实现云计算服务器与网络中其他网络的边界防护与入侵防范等。

- 安全区域边界：通过安全设备及网络设备合理划分

安全域：云数据中心

为内部区域，其它为外部区域，通过在核心交换机上部署入侵检测系统(IDS),实现发现访问控制过程中的威胁并及时做好防护策略；通过旁路部署神探系统流量探针，采用监听与智能分析技术，对系统的控制、采集请求，数据库存取、系统运维等关键行为进行审计，对攻击及时预警；在内部用户网络边界部署下一代防火墙配合入侵防御模块（IPS），实现内部用户终端到云服务器区的访问控制，对云服务器的安全起到安全保障;在互联网边界,通过部署入侵防御系统(IPS)实现对原有外部边界防火墙的功能互补，抵御来自互联网的攻击，通过部署蜜罐设备及时发现来自互联网的威胁,将威胁攻击诱捕至蜜罐,从而让安全运维人员及早发现黑客的攻击行为与手段,提前做出预判并提升安全防护等级，也为安全防护策略的建议争取宝贵的时间，从而满足等保中安全区域边界的要求。

- 安全计算环境：通过部署六方云池，采用流量引流或镜像的接口，通过

云池平台上包含的各类安全组件来实现防护;通过在云主机安装云主机防护软件，实现对终端主机的防护，满足等保中安全计算环境的相关要求。

- 安全管理中心：以神探系统分析平台作为辅助安全管理中心，实现对网

络流量的统一采集、分析及主要防护设备的统一运维，形成云数据中心的安全运营中心，统一维护日常的信息安全防护，对安全事件的应急处置、攻击行为的发现提供技术支撑。

（2）热轧工业控制系统安全防护建设

工业控制系统安全防护设计应以构建可持续演进的、能主动发现隐患并支持智能决策的安全防护能力为目标。为实现这一目标，不能单纯依赖技术手段、安全软硬件设施的简单堆叠，而应当采用先进的安全技术、构建全天候的安全运营体系、并落实因地制宜的安全管理制度。其中，安全运营是衔接技术手段和管理制度，并让安全防护能力持续有效的核心。

在安全技术、安全运营能力及安全管理制度的落实中，必须考虑到企业工控网络在时延敏感性、工业控制协议、工控网络架构、工业上下位机漏洞等方面的特点并有针对性的提出防护方法，总结得出关键防护原则如下：

•**分层分区：**依据“垂直分层，水平分区”的思想对工业控制系统进行细致的安全区域划分，同时根据不同区域的安全防护需求特点分安全级别的落实安全措施。

•**本体保护：**工业系统中的各个模块均应实现自身的安全。同时，在条件不具备的条件下将各模块本体作为安全防护的单元，应用必要的安全技术、管理手段和应急措施。

•**智能分析：**在构筑安全架构的基础上，通过对 AI 技术实现对网络行为中潜藏异常风险进行挖掘，通过智能化的策略建议提供更高的安全防护水平。

•**集中管控：**对部署的安全防护技术手段应在系统范围内进行集中管控，将孤立的安全能力整合成协同工作的安全防护体系。

详细拓扑如图 4-4 所示：

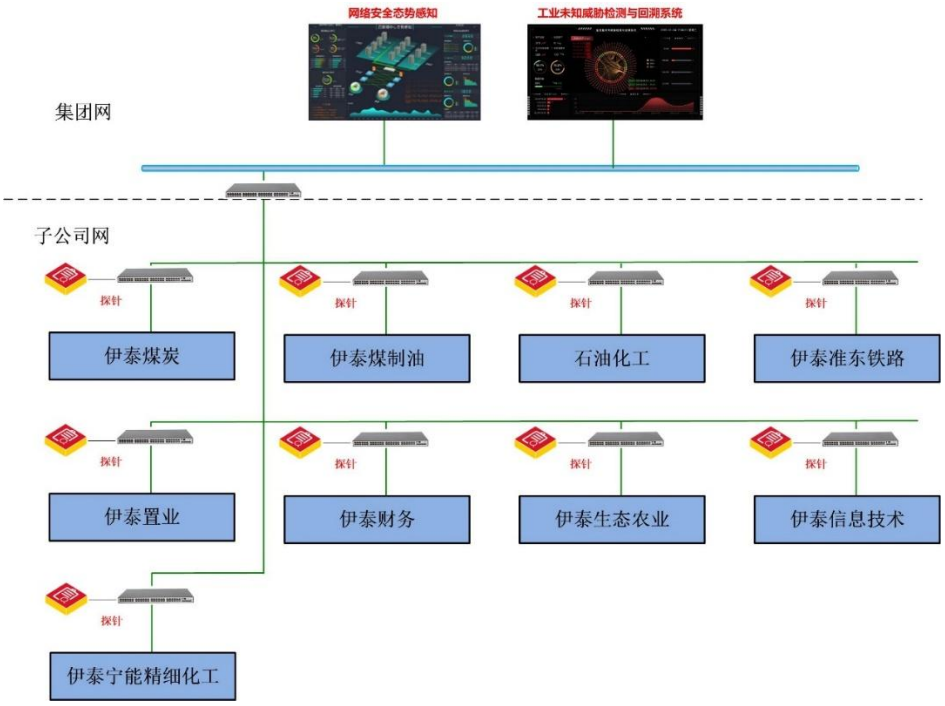

图 4-4　拓扑示意图

1.1.3　下一步实施计划

1. 计划 1

全面提升钢铁厂生产控制大区工控网络安全防护管理的合规性，符合国家主管部门、行业监管部门的管理要求以及工控安全防护要求。

2. 计划 2

通过初步安全防护实施，整体提升工控安全防护能力，提升整个工控网络实时监测预警能力以及安全运维能力；全面改善业务人员的安全水平和安全意识，提升安全管理水平、工作效率和管理效率。

3. 计划 3

实现恶意代码的监测、分析、告警、处置和管理，能够监测恶意代码网络传播和攻击行为，并采用人工智能技术进行关联分析和综合分析，有效解决静态特征码监测方式的弊端，提升全行业动态检测能力。

1.1.4　方案创新点和实施效果

1. 方案先进性及创新点

（1）打造 IT 与 OT 融合的纵深防御体系

方案设计中通过部署工业审计、智能工业防火墙、全流量未知威胁检测与回溯系统、工业卫士、监管平台产品，打造 IT 和 OT 融合的纵深防御体系。采用 IT 和 OT 数据融合技术、AI 技术、人工智能技术，基于工业大数据全流量持续监测系统中已知威胁和未知威胁。

（2）全网资产测绘以及工业行为可视化

实现工控网络资产的可视化管理，动态识别非法接入设备，直观展示工控网络安全威胁，利用丰富的可视化展现经验和技术手段。平台建设完成后将依据工业网络系统实际拓扑提供大量的监视视图。可视化视图将针对不同的展示数据，不仅提供饼状图、柱状图等形式展示对比及分布数据，利用趋势图反映周期性的监测数据，同时采用复杂算法和布局的可视化展示技术创建视网膜图、多维视图反映数据规律，增加用户对数据的可读性。

（3）极大减少运维工作量

产品采用 AI 模型进行威胁检测，从核心技术上区别于传统安全感知设备，通过安全日志 AI 聚合技术，将一类安全告警形成简洁的安全事件呈现给用户，克服了传统设备告警数量巨大、误报率高的缺点，极大地减少了运维人员的工作量。

2. 实施效果

通过一系列的安全防护建设，满足了等级保护制度对工业控制系统安全防护的要求，为客户解决生产控制系统管理难、运维难、资产看不清、资产之间访问关系和访问行为无法掌握等难题。

■ 实现网络安全态势从未知到已知

通过建立生产控制系统信息安全监管与预警平台，摸清家底，感

知网络中的资产信息，实现网络资产可视化。通过摸清家底，了解网络中存在哪些设备、对应的责任人是谁、使用什么操作系统、安装了哪些软件和应用，分别是什么组件、什么版本，分别存在哪些漏洞、已经修补了哪些补丁等等，真正做到底数清、情况明确。

■ 实现网络安全防御从被动到主动

通过建立钢铁行业生产控制系统监管预警平台，利用安全大数据、态势感知、攻击链模型和算法，结合最新的全球网络安全威胁情报，持续监测，准确及时地发现各种潜在威胁和攻击，并进行通报预警，提前感知攻击者的下一步攻击计划，采取有效处置措施，构建弹性防御体系，以期最大限度上避免、转移、降低信息系统所面临的风险。

■ 实现从单一设备防护到协同联动

通过建立生产控制系统监管与预警平台，作为联动枢纽，实现网络中所有安全设备的数据汇总分析、数据共享及策略协同，打通终端、边界协同联动，有机整合各种网络安全技术，达到“智能检测”、“智能上报”、“智能响应”，建立一个以威胁情报为驱动，终端安全、边界安全、大数据分析等多层次、纵深智能协同的安全防御体系，有效提升整体网络防护能力。

■ 实现网络安全纵深防御防护体系

通过工控系统安全防护要求，对生产控制系统网络安全进行整改加固，在坚持“安全分区、网络专用、横向隔离、纵向认证”的原则，强化边界防护的基础上，加强内部的物理安全、网络安全、操作系统安全、应用安全、数据安全防护以及安全运维管控，构建纵深防线，实现智能制造企业生产控制系统网络安全的纵深防御、综合防护。

1.1.5 单位基本信息

北京六方云信息技术有限公司是一家技术领先的“新安全”公司，

六方云借助人工智能技术仿生人体免疫机制，针对工业客户和政企客户的安全需求，创造性地提出了“AI 基因、威胁免疫”的“新时代、新安全”安全理念，采用+AI 和 AI+战略，将人工智能技术应用于全系列产品，构建安全威胁免疫系统。在国家新基建战略下，致力于提供关键信息基础设施保护、工业互联网安全的产品和解决方案，拥有保护工业客户和政企客户的“5+1”产品线：工控安全产品线、网络安全产品线、云安全产品线、安全态势感知产品线、人工智能安全产品线及安全服务。

六方云董事长任增强表示：工业互联网安全、云安全、人工智能安全是“新安全”，是未来，而未来世界发展的主要推动力来自于技术。六方云坚持以吸引和团结有共同价值观的人才为核心，持续不断地耕耘攻坚，实现“以技术保障技术”，用最先进的技术解决国家与行业在高速发展中的安全问题，保障国家工业互联网战略、云安全战略、以及新基建安全的实现，让万物安全互联。