

## 场景需求 REQUIREMENTS

煤炭是我国的最重要基础能源，占一次能源消费的70%左右。随着5G、大数据、云计算、人工智能等新一代智能化技术在矿山开采过程中的广泛应用，矿山生产网络也逐渐从封闭走向开放。随着融合一体化平台、各类智能化工作面、监控监测类业务子系统的改造建设，数据交互越发复杂，对整个矿井网络、控制系统安全也提出了更高要求。目前矿山生产系统逐步实现智能化改造，但是网络安全建设远远没有跟上信息化建设的步伐，亟需进行整体安全能力的建设，全面保障智慧矿山安全生产。



## 解决方案 SOLUTION

**加强边界隔离防护：**在安全域划分的基础上在网络边界采取隔离保护措施。生产网与办公网之间部署工业网闸实现网间的单向隔离；生产网内部调度中心到地面环网、井下环网之间部署工业防火墙，通过逻辑隔离，阻断病毒传播、黑客攻击、限制违法操作。

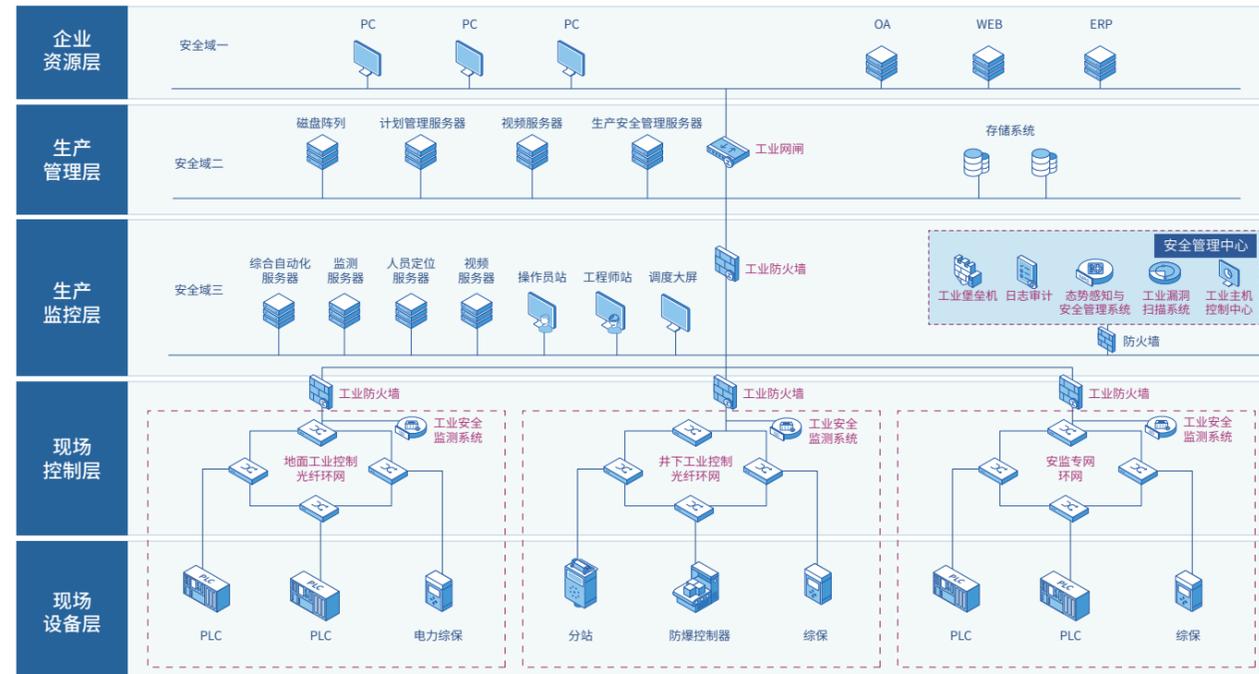
**工业主机安全加固：**在生产网各操作员站、工程师站及服务器上部署工业主机防护软件，通过应用白名单、外设管控、病毒防御、访问控制、主机加固等技术，防止病毒、木马对主机的感染，保障各系统内工业主机安全。

**生产网络安全监测：**在环网核心交换机或其它生产网流量汇聚节点上旁路部署工业安全监测系统，采集工控网络流量，深度解析数据包，生成网络行为基线，识别入侵行为、病毒攻击以及非法操作，及时告警。

**矿井运营管理中心：**部署工业安全态势感知系统，通过收集生产网内流量、日志等安全数据，结合威胁情报数据，基于关联分析引擎、异常行为分析模型，从工控资产、资产漏洞、网络威胁、操作行为等多个维度进行大数据分析，以组态化的形式将工业网络的安全态势进行可视化大屏呈现，对网络威胁及时进行应急响应，为企业安全建设升级优化提供实践依据。

**生产网络日志审计：**部署工业日志审计系统实现生产网内各类应用系统、网络设备、安全设备的日志、事件、告警集中采集与审计。

**生产网络安全运维：**部署工业堡垒机，针对煤炭生产网大量重要资产，提供统一身份认证，对资产账号及权限等进行集中化运维管控，对操作进行精准审计。



## 成功案例 SUCCESSFUL CASE

- 陕煤集团黄陵矿业
- 山西天地王坡煤业
- 晋能控股集团塔山煤矿
- 神华宝日希勒能源

## 场景需求 REQUIREMENTS

钢铁工业是我国国民经济的重要基础产业，是国家经济水平和综合国力的重要标志，钢铁发展直接影响着与其相关的国防工业及建筑、机械、造船、汽车、家电等行业，其中炼铁、炼钢、热轧、冷轧生产车间内工控系统是重点防护对象。在安全建设过程中，需从边界防护、主机防护、安全监测、安全运维、安全管理等多个角度进行设计，并结合等级保护2.0等相关标准的要求，持续加强安全监测、防护与综合运营能力。



## 解决方案 SOLUTION

**强化边界隔离防护：**在钢铁企业生产网与办公网之间部署工业网闸，实现工控网络与非工控网络单向隔离；在炼铁、炼钢、热轧、冷轧等车间产线之间的区域边界部署工业防火墙，保障各区域边界安全。

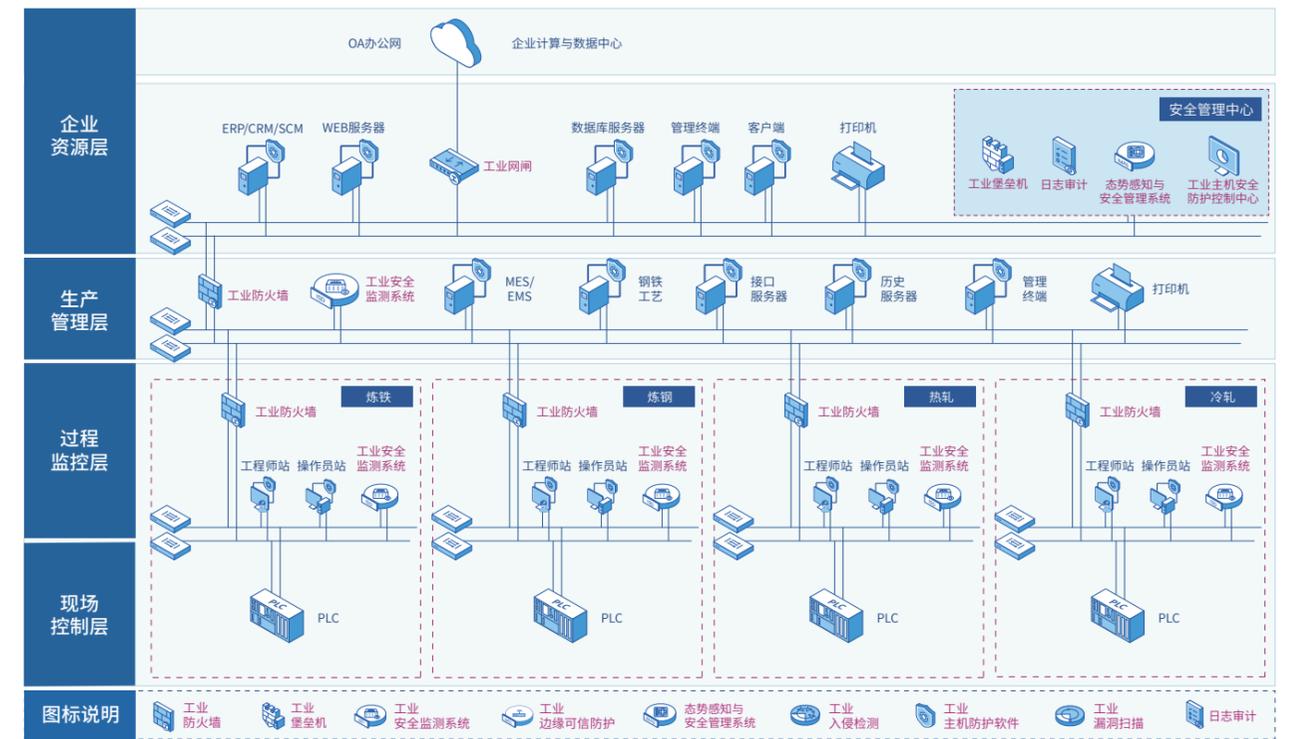
**工业主机安全防护：**对工控网络操作员站、工程师站、服务器等设备部署白名单防护软件，防止病毒、木马对主机的感染，保障各系统内工业主机安全。

**生产网络安全监测：**在各车间生产网流量汇聚点，旁路部署工业安全监测系统，自动发现工业资产，洞悉资产漏洞，深入分析网络流量，发现网络内异常操作与入侵行为，及时告警并上报态势感知平台。

**安全态势感知与集中管理：**建立安全管理中心区，部署工业态势感知系统，收集安全数据，基于关联分析引擎、异常行为分析模型，从资产、漏洞、威胁、行为等维度，分析展现全局网络安全态势。

**安全审计与安全评估：**部署工业日志审计系统，实现网内各类系统的日志、事件、告警集中存储与审计；部署工业漏洞扫描系统，定期实施主动扫描，发现工业资产潜在风险。

**生产网络安全运维：**部署工业堡垒机，提供统一身份认证接口，对资产及账号等进行集中化运维管控，实现对运维人员管理操作的全程审计。



## 成功案例 SUCCESSFUL CASE

- 南京钢铁集团
- 河北钢铁集团
- 包头钢铁集团
- 鞍钢股份