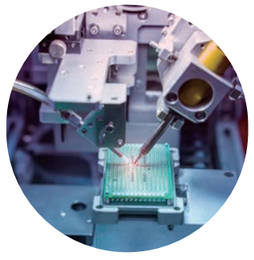
电子制造

奇安信 新一代网络安全领军者

场景需求 REQUIREMENTS



随着数字化转型与智能制造的推进，电子制造企业纷纷采取措施，在OT生产环境中利用IT技术促进信息交换，比如将MES（制造执行系统）、工业控制系统（ICS）、智能传感器、工业物联网平台（IIoT）以及数据采集与分析系统等引入到生产制造过程中，以优化业务流程，提高效率，降低成本，从而提升竞争力。然而，新技术、新应用在带来数据共享与效率提升的同时，也给电子制造行业带来了潜在的网络安全隐患，尤其以控制系统最为严重，亟需完善的工控系统安全防护方案。

解决方案 SOLUTION

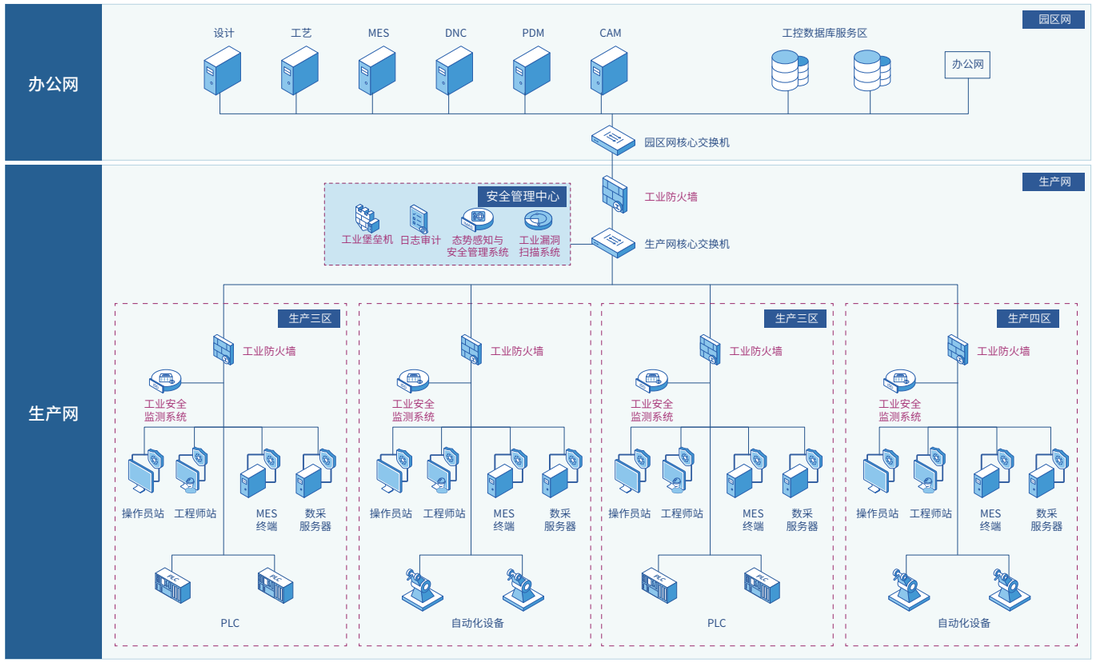
边界安全隔离：采用工业防火墙或工业网闸对生产网与管理网进行安全隔离，或者在生产网内部不同区域的边界进行隔离防护，保护生产系统免受外网攻击。

终端安全防护：电子制造行业存在大量各种计算机辅助制造、设计以及订单计划用途的工业计算机，需对此类设备进行严格的防护，通过白名单与主机访问控制策略，结合移动介质管理等手段，保障终端免受病毒攻击。

安全监测审计：电子制造行业存在大量高端机密仪器设备，部分接入生产网使用，通过实时入侵与行为监测审计，保障各种生产辅助系统及控制设备安全。

生产网络安全运维：电子制造业生产场景比较分散，多个不同工艺车间协同工作，网络与安全设备统一管理较为不易，因此采用工业安全管理分析系统，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可在执行设备统一运营管理的同时，完成安全运维数据分析。

建设安全管理中心：安全管理中心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，展示全局网络安全态势；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。



成功案例 SUCCESSFUL CASE

- 宁德时代
- 天马微电子
- 京东方
- 欣旺达电子

装备制造

奇安信 新一代网络安全领军者

场景需求 REQUIREMENTS

制造业是我国的支柱产业之一，目前大部分重型装备制造行业企业的车间已完成信息化、网络化转型，正在逐步探索尝试智能化无人工厂。装备制造行业普遍采用MES、ERP等信息化手段提升生产效率，大量使用联网智能机器臂、AGV、精密机床。随着工业互联网的发展，设备联网，应用上云，原本的信息孤岛被打破，随之而来的则是来自互联网的各种威胁，做好工业控制系统安全防护迫切而重要。

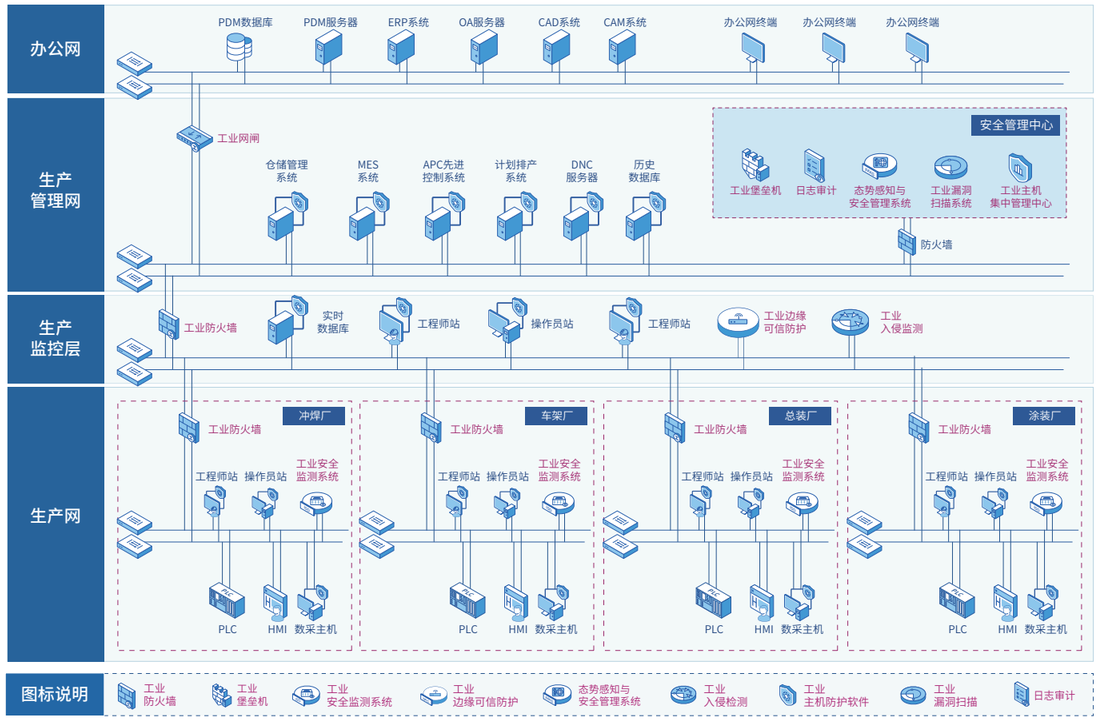
解决方案 SOLUTION

边界安全防护：对园区工厂进行最小域划分，采用工业防火墙或工业网闸对两网边界进行隔离，在生产车间边界通过工业防火墙完成横向保护，在机床前置CNC防护装置进行设备防护。

终端安全防护：智能装备制造行业存在大量数量机床，对数控机床USB接口进行拆除，对无线、CAM、MES及其他终端进行白名单防护及移动介质管控，对各类工程师、操作员站点进行访问控制限制、白名单加固及移动介质管理，保障终端安全。

安全监测审计：智能装备制造的环境中，存在大量非法授权接入、非法外联及异常工艺操作，为保障各类辅助系及控制设备安全，在各车间及生产园区核心节点部署工业安全监测与审计设备，对各类资产进行实时监控保护。

安全运维与管理：在管理中心部署工业安全态势感知与管理分析平台，对分散在各地域及各工厂的全量资产进行监控保护，对各车间发生的工艺行为、存在的资产漏洞、威胁入侵、非法接入等信息进行集中分析，为决策者提供可视化的实时平台，大幅提升安全运维与管理效率。



成功案例 SUCCESSFUL CASE

- 比亚迪
- 三一重工
- 新特能源
- 长安福特汽车