

场景需求 REQUIREMENTS

近年随着我国各大城市地铁建设速度加快，国内已开通轨道交通服务的城市共有47个。在众多轨道交通系统中，ISCS综合监控系统承担了城市轨道交通统一指挥管理，各专业系统之间信息互通、资源共享的重要职能，是重点防护对象。在安全建设过程中，应依据网络安全法、数据安全法、等级保护相关安全要求，提高轨交控制系统安全防护、实时监测与综合运营能力，保障城市轨交安全运行、市民安全出行。



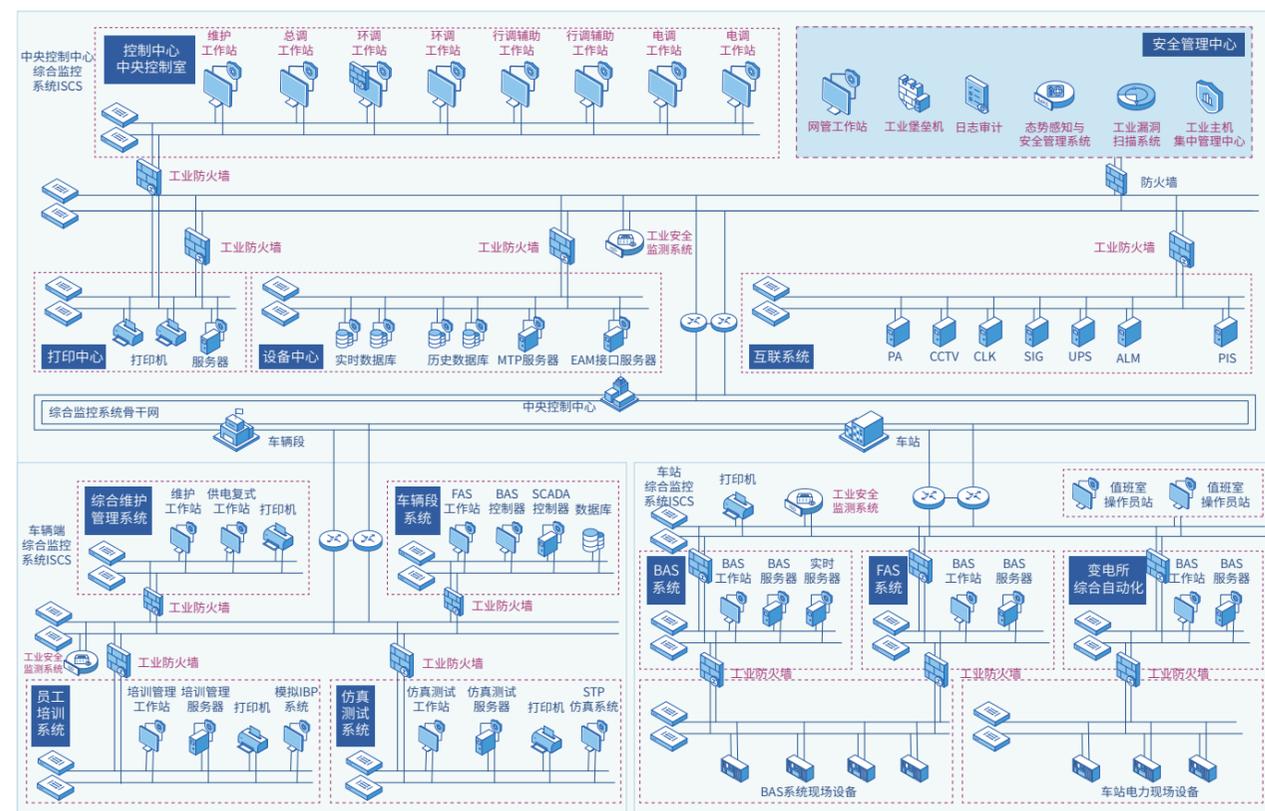
解决方案 SOLUTION

强化边界安全防护:在中央控制中心ISCS与地铁线网中心、OA系统、电力调度、PIS、PA、AFC等网络边界、站ISCS与其它专业系统SIG、PIS、AFC、PSD、ACS、PA、CCTV等系统边界，在车辆段/停车场ISCS与其它专业系统的边界部署工业防火墙，实现协议白名单管控、访问控制、入侵防御和病毒防御。

工业主机安全加固:对各区域内 在操作员站、工程师站、服务器部署工业主机防护系统，防护各恶意软件。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，保障各系统内主机安全。

流量监测与审计:旁路部署工业安全监测系统，自动发现工业资产，洞悉资产脆弱性风险；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。

建设安全管理中心:在中央控制中心建立安全管理中心区，部署工业安全态势感知与管理平台，实现设备集中管控及安全态势展示；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；部署工业漏扫，实现实时在线漏洞扫描；部署工业日志审计，实现网内各类系统、数据库的日志、事件、告警统一收集与监控。



成功案例 SUCCESSFUL CASE

- 福州地铁六号线
- 长沙地铁六号线
- 合肥地铁四号线
- 西安地铁五号线

场景需求 REQUIREMENTS

港口行业是国家关键基础设施的重要组成部分，中共中央、国务院印发《交通强国建设纲要》、《关于建设世界一流港口的指导意见》等相关政策，要求建设世界先进的世界一流港口。港口场景中岸桥、场桥、5G无人驾驶集装箱货车等业务控制系统是重点防护对象。在安全建设过程中，应结合网络安全法、等级保护、关基保护相关要求，持续提高安全防护、实时监测与综合运营能力，保障国家重要港口枢纽安全运行。



解决方案 SOLUTION

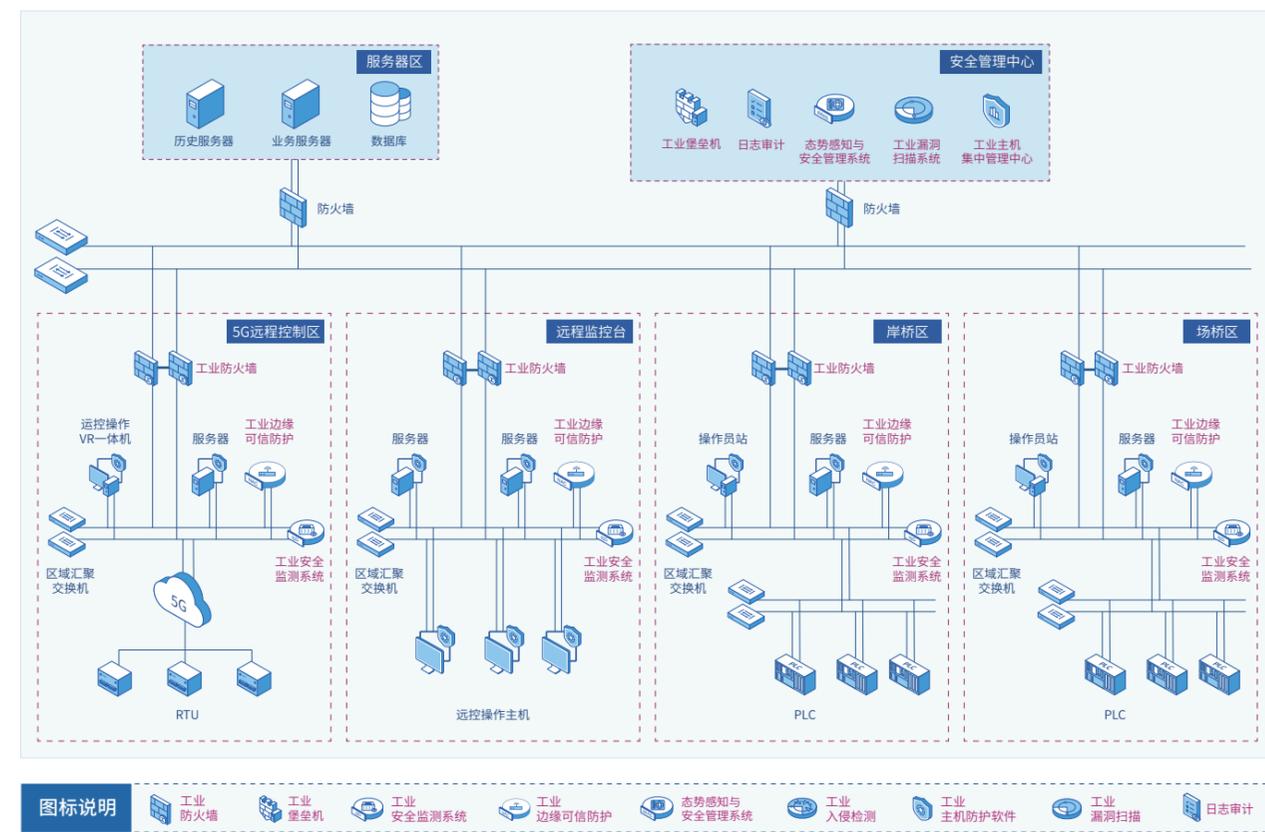
网络边界隔离防护:在岸桥、场桥与远程监控台/TOS/服务器区之间部署工业防火墙，实现协议白名单管控、访问控制、入侵防御和病毒防御，为保障控制系统稳定和可靠性，工业防火墙采用双机热备部署。

工控协议流量监测:在岸桥、场桥控制系统核心交换机分别旁路部署工业安全监测系统，自动发现工业资产、工控漏洞，洞悉资产脆弱性风险；深入分析工控网络协议流量，发现网络内异常操作与入侵行为，及时告警并上传工业态势感知平台。

安全运营管理中心:建立安全运营与管理中心，部署工业安全态势感知平台，收集安全数据，基于关联分析引擎、异常行为分析模型，从工控资产、工控漏洞、工控行为、威胁等多个维度进行关联分析，展现全局网络安全态势，预测未来发展趋势，便于领导决策研判。

系统日志实时审计:部署工业日志审计系统实现网内各类系统的日志、事件、告警集中存储与统一审计。

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。



成功案例 SUCCESSFUL CASE

- 天津港智慧码头