# 应用案例｜某市轨道交通6号线工程信号系统项目





·  
·  
  
·  
  
·**一项目背景**

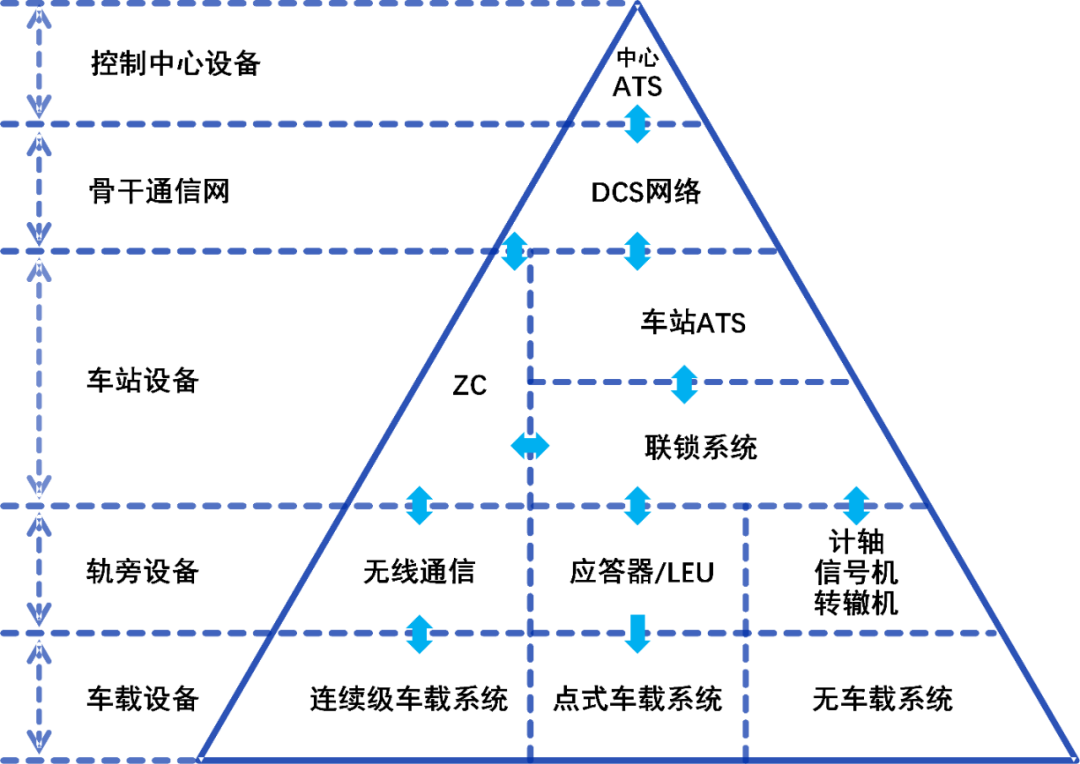
随着我国城市化进程的不断加快，城市基础设施特别是城市交通与城市发展的矛盾逐渐显现，城市轨道交通对整个城市的总体规划、促进和引导沿线规划建设和经济发展、改善城市公共交通状况、优化城市交通结构等方面都起到了积极作用，同时轨道交通系统也是现代城市交通的主流和方向，其大容量、高速度、干扰小、能耗低、被誉为现代城市的大动脉，是城市进入国际现代城市交通的重要标志，也是解决城市交通紧张的最有效途径。

本案例轨道交通6号线为东西向骨干线路，快速衔接城市副中心、城市主中心、开发区南部、空港和机场，加强城市“一主两次”跨区联系，引导城市东西向拓展。工程西起国际新城，东至机场，线路全长近50km，并预留继续往东延伸至新航站区的条件。该线全为地下线，设车站34座，全为地下站，其中换乘站13座，与地铁1、2、3、4、5、7、8、9、12号线换乘，与规划中的两条城际线、机场线换乘。在线路西侧起点设有停车场，在线路东侧附近设车辆段检修基地；与其它两条线路共享主变，同时新建第二控制中心。6号线自西向东经过了5区1县6个行政区，起到了加强城市各区之间的快速联系、协调发展的重要作用。

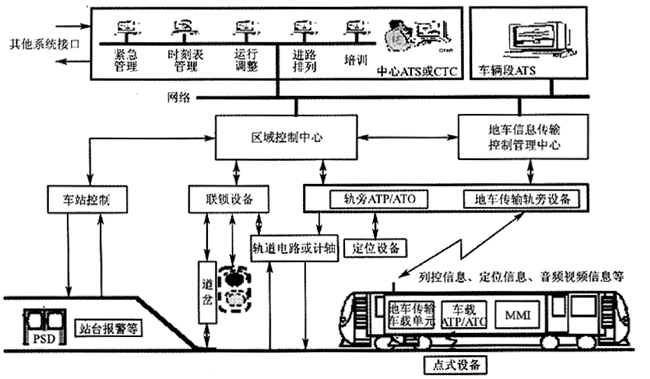
**二现状分析**

**信号系统**

城市轨道交通信号系统通常由列车运行自动控制系统（ATC）和车辆段信号控制系统两大部分组成，用于列车联锁、进路控制、列车间隔控制、调度指挥、信息管理、设备工况监测及维护管理等方面，由此构成一个高效综合自动化系统。城市轨道交通信号系统是保证列车运行安全，实现行车指挥和列车运行现代化，提高运输效率的关键系统。



项目技术规格书中的需求显示，6号线信号系统应按照《信息安全等级保护管理办法》（公通字[2007]43号）、《中华人民共和国计算机信息系统安全保护条例》（国务院令第147号）和《信息系统安全保护等级保护实施指南》（GB/T25058-2010）实施等级保护工作，应符合国家安全部门对信号系统中DCS子系统应满足信息安全等级保护标准三级的要求，系统能够防范病毒入侵、黑客攻击、对数据有审计功能等技术要求的能力。信号系统应接受并通过信息保护等级相适应的测试，并在试运营前通过等级保护测评。



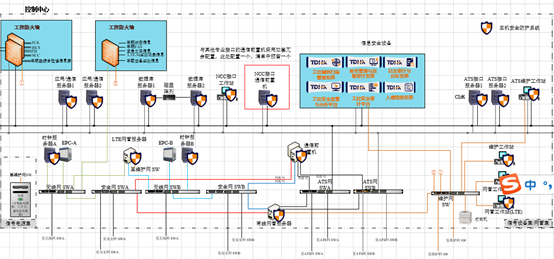
结合《网络安全法》、GB/T 22239-2019 《信息安全技术网络安全等级保护基本要求》以及轨交协团体标准T/CAMET 11001.1-2019 《智慧城市轨道交通 信息技术架构及网络安全规范》中的网络安全相关要求，总结过往项目经验，以及系统运营现场的安全现状，发现一些综合性的风险如下：

* **从业人员安全意识相对薄弱**轨道交通行业相关工作人员对信息安全方面的了解仍存在不足，信息安全标准定义模糊，容易产生信息安全危机，安全意识仍需提升。
* **对非法接入与无线攻击缺乏相应的管理手段和措施**在轨道交通站内这种公共区域，客流量很大，每天都会有海量的用户进行无线连接，这些访问请求通过各种方法和渠道来连接轨道交通内部和外部的各类无线网络信号，势必就有可能会对轨道交通内部的无线通信系统造成冲击，甚至是遭到破坏和非法攻击，进而对安全产生较大的影响。
* **服务器、工作站、终端操作系统的安全威胁**轨道交通信号系统网络由大量开放系统组成，大量的微机监测服务器、站机、终端机都采用windows操作系统。而针对Windows系统产生的项击相对较多，受到破坏的可能性就大。
* **应用软件的安全威胁**信号系统的各类设备提供商提供的应用授权版本不可做到尽善尽美，随之就会出现各种各样的后门、漏漏BUG等。
* **直接或间接来自于生产网的安全威胁**由于信号系统与其它系统存在接口，在网络边界或区域之间是否配置了访问控制策略和策略的颗粒度决定了系统受到的风险冲击或高或低，同时来自病毒和其它网络的攻击也可能对信号系统内部网络产生影响。

天地和兴结合轨道交通信号系统的普遍问题和6号线工程信号系统的实际情况，针对可能存在的风险，提出了具有针对性的网络安全解决方案。

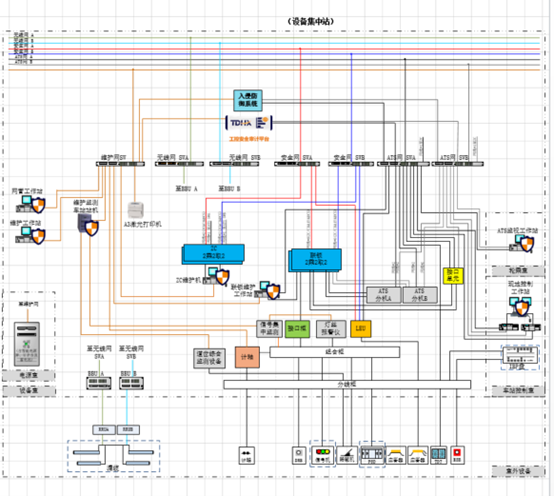
**三解决方案**

**控制中心**



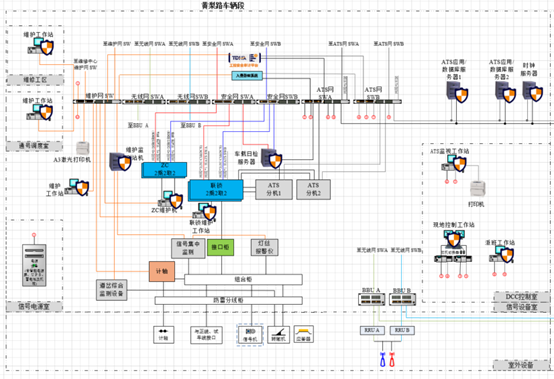
部署的产品和服务：工控防火墙、工控安全审计、入侵检测系统、主机安全防护系统、主机安全加固服务、账号管理及运维审计系统、日志审计与分析系统、工控漏洞扫描管理系统、工控信息安全监管与分析平台。

**设备集站中心**



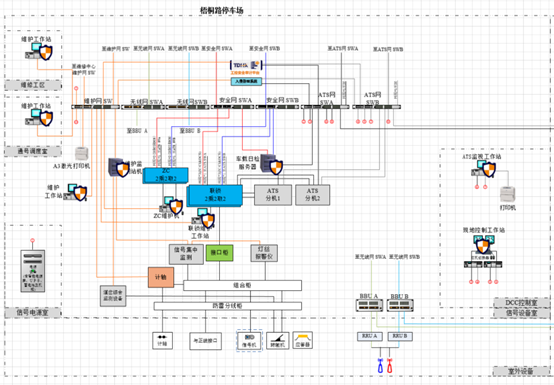
部署的产品和服务：工控防火墙、工控安全审计、主机安全防护系统、主机安全加固服务。

**车辆基地**



部署的产品和服务：工控安全审计、主机安全防护系统、主机安全加固服务。

**停车场**



部署的产品和服务：工控安全审计、主机安全防护系统、主机安全加固服务

防火墙：按照最小化原则配置访问控制策略。实现区域逻辑隔离，通过IP/MAC绑定、建立边界访问黑白名单等安全策略，建立不同安全域之间的访问控制策略，确保非授权的设备不能在内外网之间随意连接，避免在一个系统或区域里爆发的工控安全事件扩散到其他系统或区域当中，保障区域间通信网络安全。

工控安全审计系统系统：对整个信号系统的应用服务器、主机管理系统等进行全面的检测，对通信传输网络内的数据进行合规性检查，对异常行为、违规操作行为进行识别、审计告警，告警日志送日志审计系统、安全管理平台系统进行集中存储、分析与风险关联展示，辅助安全运维人员进行处置。

入侵检测系统：对网络出入口、重要安全域的通信数据进行实时检测，用于识别监控网络中可能存在的各种已知攻击行为，并进行审计告警，告警日志送日志审计系统、安全管理平台进行风险分析与可视化，辅助安全运维人员进行风险处置。

主机安全防护系统：在信号系统全线的关键服务器、工作站和终端上部署，可有效的实现主机防病毒、防第三方软件的非授权安装与使用，主机系统外接口的管控，USB外接存储设备的认证管控、防病毒与操作行为审计，为主机系统安全运行提供必要的安全保障。

安全加固服务：针对信号系统内所有上位机、网络设备以及服务器等进行符合等级保护要求的人工加固服务，主要工作包括：完成所有服务器、工控机、主机的未使用的USB接口、串行口、无线、蓝牙、光驱等关闭工作；完善操作系统、数据库、应用系统口令长度及复杂度，配置用户登录失败处理机制等。

账号管理及运维审计系统：部署在安全管理域内，通过代理模式部署，作为系统运维的统一入口，实现系统运维权限统一认证管理以及操作行为审计。

日志审计与分析系统：部署在安全管理域内，主要通过syslog、SNMP等方式、或通过代理方式收集网络中各系统产品的告警日志，进行日志的集中存储、范式化与安全分析与展示。

工控漏洞扫描管理系统：对整个信号系统进行全面的漏洞扫描和安全风险评估，将扫描的漏洞结果导入工控集中监管与审计系统，帮助运营工作人员发现网络和应用中存在的配置缺陷、管理漏洞，提升网络和应用系统的安全强度。

工控信息安全监管与分析平台：部署在安全管理域内，以实现对信号系统全网安全系统的状态监控、安全风险的集中收集、存储、关联分析与可视化、安全风险集中处置等集中安全管理功能，工控信息安全监管与分析平台是整个信号系统网络安全防护体系的安全大脑，是安全管理域的核心平台系统。

**四应用价值**

通过采用一整套的工控系统信息安全解决方案，以建立纵深防御策略为主要思想，在保证建立立体化防护的同时，构建了一个以信号系统为中心的空间综合防控系统，并尝试研究和绘制了信号系统网络空间信息图谱，提升了系统的安全防御能力和水平。

**区域隔离：**工控防火墙隔离和过滤了两个区域网络间的通信，使得风险被控制或限制在最初发生的区域内，而不会影响到其它部分；

**深度检查**：面向应用层对特有的工业通讯协议进行内容深度检查，告别病毒库升级缺陷；

**通信管控：**通信规则是可以通过中央管理平台进行在线组态和测试的；

**数据审计：**完善的安全审计平台，对网络运行日志、操作系统运行日志、安全设施运行日志等进行集中收集、自动分析，及时发现各种违规行为以及病毒和黑客的攻击行为；

**威胁检查：**部署于网络边界的威胁检测系统能够快速准确发现入侵监控系统的病毒和恶意代码，并实施清除并报警。

**实时报警：**所有部署的工控信息安全防护产品都能由管理平台统一进行实时监控，任何非法的（没有被组态允许的）访问，都会在管理平台产生实时报警信息，从而故障问题会在原始发生区域被迅速的发现和解决。