# 应用案例｜某市轨道交通某线一期工程全自动运行系统项目·****一项目背景****

城市轨道交通是以电能为动力，是采取轮轨运输方式的快速大运量公共交通的总称，是人类城市建设史上最大的公益性基础设施之一，是城市公共交通的主干线、客流运送的大动脉。仅国庆假期期间，轨道交通客运量排名靠前的十座城市，累计完成了客运量约2.2亿人次，充分显示了城市生命线工程的便捷、高效和快速的特点。



某市轨道交通5号线远期规划为环线，是该市轨道交通第二轮建设规划中的重要项目之一，5号线一期工程全长近30公里，设站20余座（换乘站10余座），起到了加强城市东西向、南北向重要发展轴之间的快速联系的重要作用。

**二现状分析**

综合监控系统（Integrated Supervision and Control System）是对城市轨道交通线路中机电设备进行监控的分层式计算机集成系统，是最重要的业务系统之一。综合监控系统集成和互联了日常运营的众多业务系统，集成对象通常包括：PSCADA、电能质量管理系统、BAS、PSD、FAS（含区间隧道感温光纤）、车站安检系统、电气火灾报警系统、消防电源监视系统、段场防火门监控系统、可视化接地等；互联对象：ATS、CCTV、PA、PIS、AFC、ACS、通信集中告警系统（TEL/ALARM）、时钟系统（CLK）、车辆调度管理系统、段场智能运维管理系统等。

通常情况下综合监控系统的硬件分为两层：中央级综合监控系统和车站级综合监控系统；网络分为三层：主干层、局域层和现场层，系统结构主要有C/S 结构或 B/S 结构两种。



典型的综合监控系统拓扑图

根据技术需求书中的要求，5号线一期工程综合监控系统（含综合监控系统及其集成子系统）信息安全应符合国家和省市信息安全相关规章及文件的要求，对整个综合监控系统进行安全配置、监控和管理，使综合监控系统能够有效识别出系统中存在的病毒危害、非法操作、异常事件和外部攻击等威胁，具备防范网络入侵、黑客攻击、安全审计、信息安全统一管理等技术要求的能力。

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“系统自保、平台统保、边界防护、等保达标、安全确保”的网络安全相关要求和轨道交通综合监控系统的特点，总结和分析了可能存在的脆弱点，如下：

系统与其他网络区域之间未采取可靠的技术隔离手段。

网络边界或区域之间未根据访问控制策略设置访问控制规则。

未在关键网络节点处对恶意代码进行检测和清除，未维护恶意代码防护机制的升级和更新。

未限制终端接入地址范围。

未提供登录失败处理措施和连接超时自动退出功能。

未限制默认账户的访问权限。

结合5号线一期工程综合监控系统和实际情况，针对可能存在的风险，提出具有针对性的解决方案。

**三解决方案**



**分区分域**

### 根据系统结构将5号线一期工程综合监控系统域分为控制中心子域和车站子域。

控制中心是独立的业务大区，主要对全线设备的实时集中监控功能和各系统之间协调联动功能两大部分。

根据区域内的业务模块和功能职责划分逻辑子区域，其中包括：外部接入区、业务服务器区域、核心交换区、运维管理区。

**中央级**
**外部接入区**

在中央级综合监控系统的网络边界部署工控防火墙

#### ****核心交换区****

在中央级综合监控系统关键节点部署工控安全审计系统

#### ****运维管理区****

为综合监控系统部署工控安全检查工具

#### ****服务器区****

为中央级综合监控系统里的服务器、工作站、操作员站部署白名单主机防护系统

**车站级**

#### ****车站****

在车站级综合监控系统网络边界部署工控防火墙

在车站级综合监控系统里的工作站部署白名单主机防护系统。

#### ****车辆段****

在车辆段的FEP边界、维修管理系统和培训管理系统分别部署工控防火墙。

在车辆段工作站上部署白名单主机防护系统。

#### ****停车场****

在停车场的网络边界部署工控防火墙。

在停车场工作站上部署白名单主机防护系统。



**工控防火墙**：将综合监控系统与外部系统，如PIS、CCTV、PA系统等子系统及统一安全管理中心进行安全隔离；提供综合监控系统与外部系统、统一安全管理中心网络边界处端口级的访问控制功能，并对综合监控系统应用层协议进行内容过滤，防止重要网段的地址欺骗；检查外部用户的非法联接内部网络及内部网络用户私自外联，并能定位及有效阻止内、外部用户非法联接。

**工控安全审计系统系统**：监视并记录对综合监控系统数据流量各类操作行为，通过对网络数据的分析，实时地、智能地解析对数据库服务器的各种操作，并记入审计数据库中以便日后进行查询、分析、过滤，实现对目标系统的用户操作的监控和审计。

**白名单主机防护系统**：可由安全管理工作站上部署的管理端统一管理，进行权限推送，在受控情况下完成日常软件和配置变更操作，防止木马、病毒等未授权软件的运行。

**工控安全检查工具**：对整个综合监控进行全面的漏洞扫描和安全风险评估。支持将扫描的漏洞结果导入工控集中监管与审计系统。

**四应用价值**

提升了5号线一期工程综合监控系统的信息安全防护能力，依据项目实施情况建立一整套技术标准和规范，推动和促进项目成果在行业、专业内的应用与实践。

方案应用了基于工业控制系统的防护手段，构建了安全可控为目标、监控审计为特征的轨道交通综合监控系统新一代主动防御体系，提升了综合监控系统整体安全性。

方案采用基于白名单机制的安全防护技术及产品来设计构建安全防护体系，借助工业控制协议的深度解析与人工智能学习技术的应用，以全面的工业漏洞库为支撑，使安全防护产品更具有基于行为的主动防御能力。安全防护体系更加贴近轨道交通行业生产控制系统环境应用，安全防护更加准确，在保证稳定性要求的同时，效率更强，使用价值更高。

方案设计参照国家等级保护相关规范要求，项目建设后将达到轨道行业等级保护的技防要求，配合轨道交通安全管理体系的规范化建设，技防配合人防促进国家等级保护对工业控制系统网络安全合规性，为轨道交通行业生产控制系统的安全保驾护航。