1.1 案例五：地铁智慧车站运营管控平台信息安全防护方案——为“智慧出行”保驾护航，实现智慧车站安全运营

1.1.1 方案概述

中国拥有全球规模最大的高铁和地铁线路网。车站是线路运行中的重要节点，是乘客输送不可缺少的场所。因此，要使轨道交通稳定、安全、高效地运行，对车站进行智慧设计和安全防护至关重要。智慧车站运营管控平台包括车站既有综合监控系统、智能视频分析系统、客流分析预测系统、实时定位系统、站务巡视系统、站务单兵系统、智慧消防系统等，并对车站既有系统进行升级。北京六方云信息技术有限公司依托实际案例，对智慧车站运营管控平台可能面临的安全风险进行研究，并针对性的提出切实落地的地铁智慧车站运营管控平台安全防护方案，在降低网络安全风险隐患的同时，满足网络安全等级保护合规性要求。

1. 方案背景

目前地铁站管理依然依靠车站人员进行人工管理，需要耗费大量人力资源，管理效率不高，难以继续提升。另外，对于特殊场景下，依靠既有设施、装备进行应对时，对车站人员各项要求依然较高。因此需在地铁站既有系统上增设智慧车站运营管控平台，包括车站既有综合监控系统、智能视频分析系统、客流分析预测系统、实时定位系统、站务巡视系统、站务单兵系统、智慧消防系统等系统，并对车站既有系统进行升级。主要解决车站站务人员工作过程中的难点、痛点，实现全面提升乘客服务质量，提高车站管理工作效率，同时为运营分公司的安全运营生产提供决策支持。业务系统与轨道交通规章制度相配套，建立一套程序化、网络化、可视化、标准化的智慧车站运营管

控平台，保障车站运行安全，提高车站运营效益，提高站务人员工作效率、降低运行成本，实现安全、高效率、低成本的运营目标。

在智慧车站运营管控平台的建设应用中，信息安全风险随之而来。运管平台以站级 ISCS 为基础，利用物联网、视频智能分析技术，实现车站态势全息感知，将设备状态与报警等自动化数据（生产网）和智能视频、运营管理、设备维保、客运服务等信息化数据（管理网）深度融合，通过大数据、人工智能进行挖掘分析、综合利用。运管平台信息安全风险主要包括管理网的公网通信风险、运管平台服务器及工作站主机安全风险、运管平台与内部 ISCS/PIS/CCTV 数据接入风险等。因此针对地铁智慧车站运营管控平台可能存在的信息安全问题进行研究，输出信息安全防护专题方案，在为运营管控平台提供信息安全保障的同时，使运营管控平台信息安全满足政策合规性，达到等保二级防护水平。

2. 方案简介

在地铁站既有系统上增设智慧车站运营管控平台并针对性进行网络安全建设，运营管控平台包括车站既有综合监控系统、智能视频分析系统、客流分析预测系统、实时定位系统、站务巡视系统、站务单兵系统、智慧消防系统等系统，并对车站既有系统进行升级，实现全面提升乘客服务质量，提高车站管理工作效率，同时为运营分公司的安全运营生产提供决策支持。运管平台以站级 ISCS 为基础，利用物联网、视频智能分析技术，实现车站态势全息感知，将设备状态与报警等自动化数据（生产网）和智能视频、运营管理、设备维保、客运服务等信息化数据（管理网）深度融合，通过大数据、人工智能进行挖掘分析、综合利用。

对智慧车站运营管控平台可能面临的安全风险进行研究，依据

“一个中心，三重防护”的安全理念，进行针对性的网络安全建设，在边界安全防护产品防火墙的应用上采用 NAT 技术，增强了网络安全产品与业务系统的黏性，整体网络安全建设完成后，提升了运营管控平台的信息安全防护能力，同时使运营管控平台信息安全满足政策合规性，达到等保二级防护水平。

3. 方案目标

（1）提高车站运营效益，提高站务人员工作效率、降低运行成本，实现安全、高效率、低成本的运营目标；

（2）提升运营管控平台的信息安全防护能力，同时使运营管控平台信息安全满足政策合规性，达到等保二级防护水平。

1.1.2 方案实施概况

运管平台以站级 ISCS 为基础，利用物联网、视频智能分析技术，实现车站态势全息感知，将设备状态与报警等自动化数据（生产网）和智能视频、运营管理、设备维保、客运服务等信息化数据（管理网）深度融合，通过大数据、人工智能进行挖掘分析、综合利用。本方案针对智慧车站运营管控平台的网络安全建设，主要为提升运营管控平台网络安全防护能力，并达到等保二级防护水平。

1. 方案总体架构和主要内容

（1）方案总体架构

根据自动化、信息化数据流向、系统接口情况以及系统功能，将运管平台系统划分为三个安全域：工业互联网接入区域、运管平台核心区域、生产内网接入区域。

在不同区域边界部署硬件防火墙，在不同系统之间制定访问控制策略，实现安全域的访问控制和区域隔离；

在运营平台核心区域部署入侵检测，对内部网络安全状况进行实

时监测；

在运管平台服务器、工作站需部署终端防护软件系统，保障终端主机安全运行；

在每个智慧车站构建安全管理中心，由统一管理平台、漏洞扫描系统、运维审计与管理系统以及日志审计系统组成，实现集中管理、统一运维、自检自查等功能。

总体网络架构如图 5-1 所示：

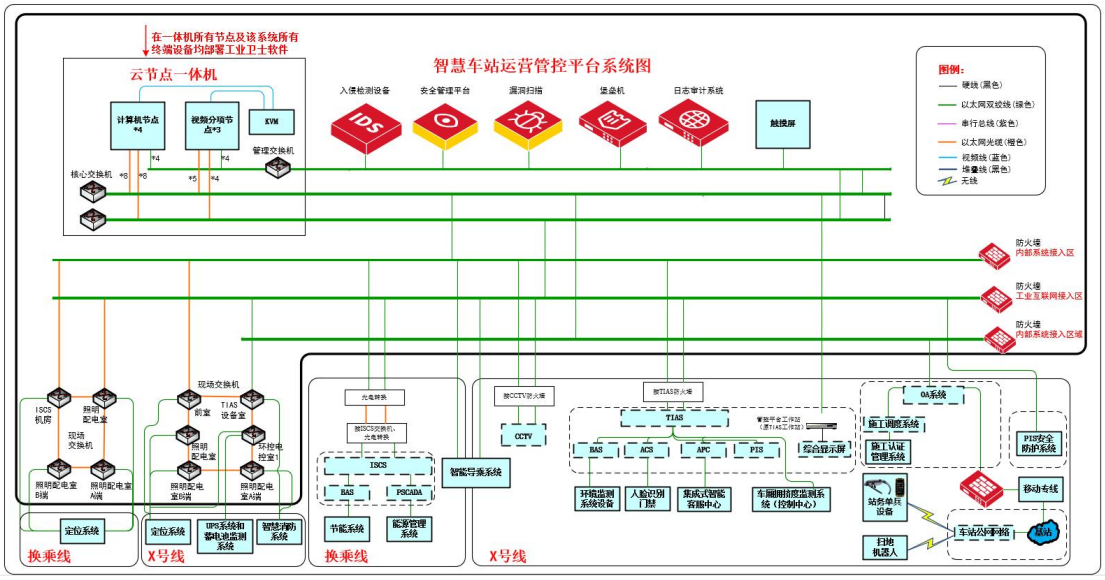

图 5-1　总体网络架构图

（2）主要内容

本方案按照“一个中心、三重防护”的核心思想进行网络安全方案设计及建设，主要应用产品包括防火墙、入侵检测、统一监管平台、漏洞扫描系统、运维审计与管理系统、日志审计系统及工业卫士软件等，具体应用及防护情况如下：

➢ 安全区域边界

将运管平台系统划分为三个安全域：工业互联网接入区域、运管平台核心区域、生产内网接入区域。在生产内网接入区域至运营平台核心区域，工业互联网接入区域至运营平台核心区域的边界部署硬件

防火墙，不同系统之间制定访问控制策略，实现安全域的访问控制和区域隔离。

基于数据流进行梳理分析，智慧车站运营管控平台需接入 TIAS 系统，该平台功能上设计为站级 TIAS 系统的上位系统，即通过该平台实现对 TIAS 中综合监控部分的设备监控；网络上，该系统需要在本站访问 TIAS 服务器、FEP，并通过 TIAS 环网分别访问主控、备控的 TIAS 实时服务器（机电）、FEP，以及实现两个及以上车站的运营管控平台网络互通（仅限于一体机的部分业务虚拟节点），传输内容为常规综合监控监控数据，不含视频流。智能扫地机器人、站务单兵设备、手持移动终端、监控平板（均设置静态 IP）通过无线与车站公网连接，车站公网通过控制中心公网与控制中心 OA 系统的接口实现上述设备与车站 OA 系统的通信。

基于业务系统访问需求进行分析，防火墙设备在进行边界防护的同时需要起到网络互联互通作用，增强信息安全设备与业务系统的黏性。增加与 TIAS 系统连接的外接口地址（由 TIAS 系统提供），防火墙内部接口地址由运营管控平台提供；通过防火墙路由模式实现内外接口通信，由于 TIAS 网络中无运营管控平台的 IP 网段，所以防火墙还需要做端口映射配置，用来对数据包目的地址进行转换实现多个站之间的平台一体机网络互通。

- **安全通信网络**

智慧车站运营管控平台的安全通信网络保障通过入侵检测系统的部署实现，入侵检测通过旁路模式部署，通过交换机镜像流量方式获取数据源进行分析，根据业务需求，入侵检测系统部署在运营平台核心区域。

- **安全计算环境**

智慧车站运营管控平台的安全计算环境通过在终端安装工业卫士实现，在运管平台服务器、工作站需部署终端防护软件系统，保障终端主机安全运行。工业卫士软件是六方云基于“白+黑”技术开发的主机防护产品，一款专门解决工业互联网中工业主机日益严重的信息安全问题，同时又完全适应工业互联网环境的一款安全防护产品。能够对工业互联网中的工程师站、操作站、SCADA 服务器、历史服务器、OPC 服务器、接口机等工业主机进行全面的安全防护。

本产品采用“白+黑”的防御策略，保证只有经过认证的软件才可以运行，其他病毒、木马、违规软件都被阻止。通过完善相应的加固策略，提升安全级别，实现工控主机从启动、加载、运行等过程全生命周期的安全保障。从而解决工业互联网中日益严重的终端安全问题。同时对 USB 端口等接口进行全面管控，U 盘等未授权设备无法接入终端计算机，有效防范通过 USB 接口发起的高级攻击。

➢ **安全管理中心**

智慧车站运营管控平台的安全管理中心由统一监管平台、漏洞扫描系统、运维审计与管理系统以及日志审计系统组成。其中，统一监管平台实现对安全事件的处置分析和对主要安全设备、软件的统一运维。漏洞扫描系统通过定期扫描的形式发现系统中存在的漏洞、问题。运维审计与管理系统对系统的运维操作进行审计和管理，规范运维过程。日志审计系统实现对日志的采集分析，满足等保合规性要求。

2. 网络、平台或安全互联架构

（1）网络互联架构

智慧车站运营管控平台需接入 TIAS 系统，该平台功能上设计为站级 TIAS 系统的上位系统，即通过该平台实现对 TIAS 中综合监控部分的设备监控；网络上，该系统需要在本站访问 TIAS 服务器、FEP，

并通过 TIAS 环网分别访问主控、备控的 TIAS 实时服务器（机电）、FEP，以及实现两个车站的运营管控平台网络互通（仅限于一体机的部分业务虚拟节点），传输内容为常规综合监控监控数据。接口界面如图 5-2 所示：

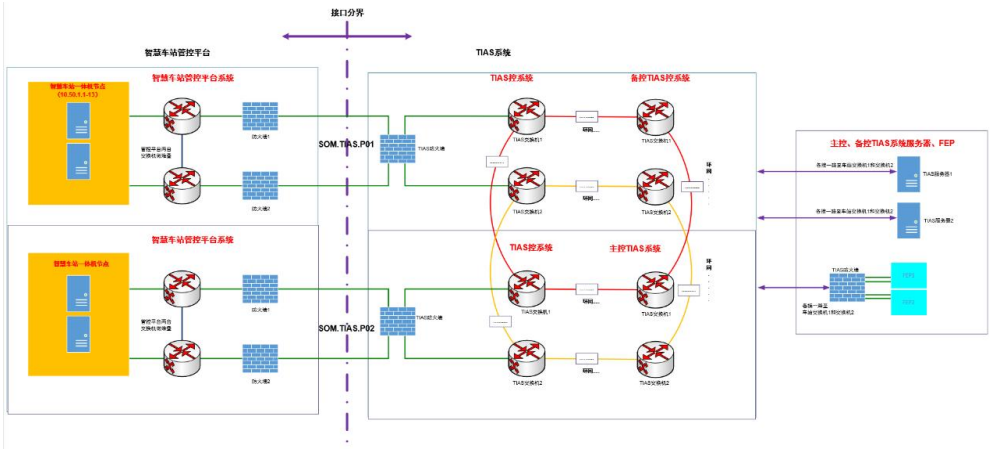

图 5-2　与 TIAS 系统接口

智慧车站运营管控平台包含了车站既有综合监控系统、智能视频分析系统、客流分析预测系统、实时定位系统、站务巡视系统、站务单兵系统、智慧消防系统等系统。其中，智能扫地机器人、站务单兵系统、车站信息管理系统、移动终端等设备需通过车站公网与 OA 网、施工调度管理系统进行连接。接口界面如图 5-3 所示：

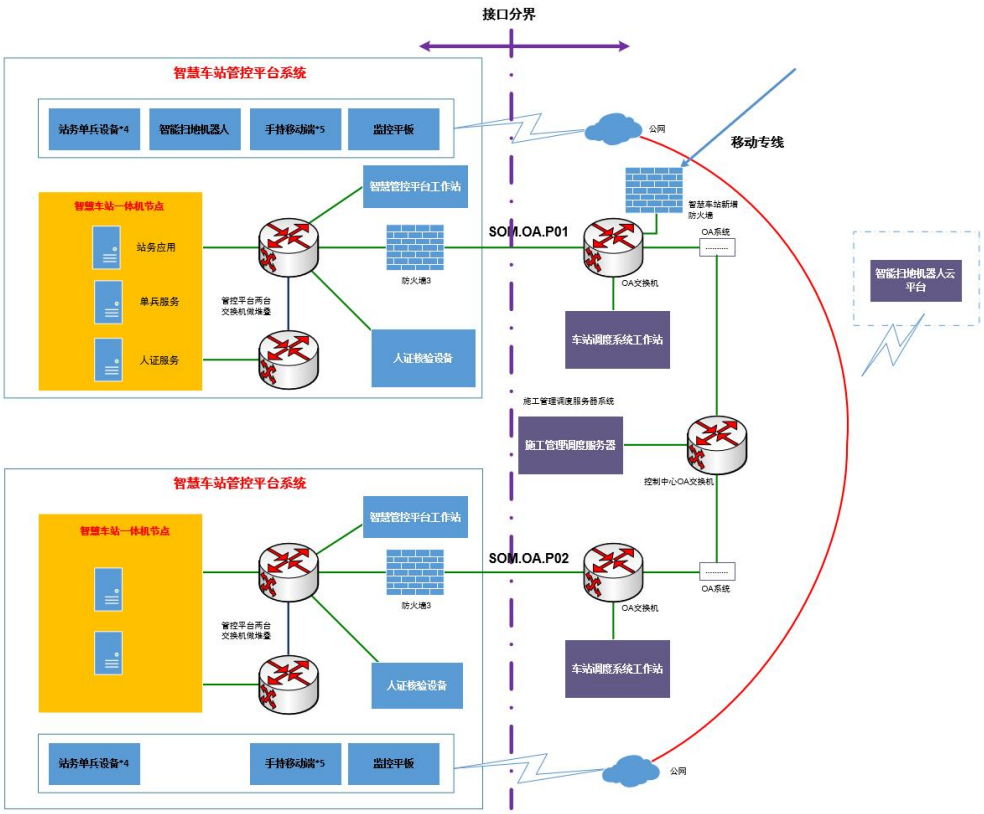

图 5-3　与 OA 系统接口

（2）安全风险

➢ 管理网风险

本系统到公网的出口是在管理网，站务巡检系统手持终端数据等需要通过公网传输。管理网与外部互联网连接，与运管平台产生数据交互，存在互联网边界安全风险。

➢ 内部系统数据交互风险

运管平台视频分析系统从 CCTV 调取视频，通过 ISCS 监控 BAS 系统部分设备，通过 PIS 系统发布电子乘务信息、电子广告。运管平台承载了自动化、信息化数据，流向比较复杂，存在横向病毒感染和传播风险。

综上所述，一旦攻击者通过管理网侵入生产网，传播糯虫病毒或恶意代码，将可能影响运管系统服务器或工作站正常工作，进而影响运管平台核心系统运行，并可能通过 ISCS/BAS 自动化数据流、

PIS/CCTV 信息化数据流侵入 ISCS/PIS/CCTV 生产内网，从而影响自控设备运行状态数据采集及指令下发。

3. 安全及可靠性

（1）主动防御：本方案在方案设计过程中，采用主动防御的安全理念，参考网络攻击步骤（侦查跟踪->武器构建->载荷投递->漏洞利用->安装植入->命令控制->目标达成），将攻击过程划分为事前、事中、事后三重维度并针对性进行网络安全防护建设：

（2）事前预防：建立一份健全的资产清单以及管理权限，应用系统漏洞检测、风险评估等技术手段对运营环境的风险特征进行描述整理，针对现有风险点可以预先采取技术加固等措施主动维护关键资产，从而最大程度地降低生命周期安全风险；

（3）事中检测/阻断：通过入侵检测/入侵防御、行为基线检查等技术手段对运营环境进行实时的持续监控和检测，为及时察觉正在发生的事件，所应用防火墙等安全产品均具备一定的运营可见性，一旦发现异常事件将第一时间进行告警推送，并能够快速阻断风险事件的进一步扩散传播；

（4）事后处置：在管理层面建立应急响应和恢复程序，在技术层面能够针对已经发生的安全事件进行日志留存、攻击取证，进而展开攻击行为分析，从而判断本次安全事件所利用的漏洞及攻击路径，并能够提供专业的处置建议，预防攻击的再次来袭。

1.1.3 下一步实施计划

1. 计划 1

本期方案建设范围仅覆盖 2 个车站，通过本方案试点建设，后续将持续推广，逐渐覆盖该线路全部车站，建设线路级智慧车站运营管控平台，并按照既有安全方案同步进行网络安全建设。

2. 计划 2

为了更好的为“智慧出行”保驾护航，在智慧车站大范围建设过程中，除基本网络安全建设外，将针对性打造安全运营中心，应用大数据、人工智能等技术实现已知威胁和未知威胁的全面检测，并提高网络安全运维效率，降低运维成本。

1.1.4 方案创新点和实施效果

1. 方案先进性及创新点

为实现智慧城市轨道交通的发展目标，传统地铁业务场景正在逐渐应用新技术进行既有线路、既有系统以及既有车站的改造升级，例如智慧车站运营管控平台建设、城轨云建设等；随着等级保护 2.0、关基保护条例等相关政策标准的推广覆盖，信息安全问题越发受到重视。依托实际案例，对智慧车站运营管控平台可能面临的安全风险进行研究，并针对性的提出切实落地的地铁智慧车站运营管控平台信息安全方案，在边界防护处增强与业务系统的黏性，可以实现针对智慧车站运营管控平台信息安全建设复制推广以及参考的作用。

2. 实施效果

全面提升乘客服务质量，提高车站管理工作效率，同时为运营分公司的安全运营生产提供决策支持。建立程序化、网络化、可视化、标准化的智慧车站运营管控平台，保障车站运行安全，提高车站运营效益，提高站务人员工作效率、降低运行成本，实现安全、高效率、低成本的运营目标。

通过事前、事中、事后多层次立体防御体系的建立，实现对车站的安全预警和防护，保证车站运营安全，预防遭受网络攻击后带来的经济损失及社会不良影响。

便于复制推广：从边界、终端、管理等多维度出发进行网络安全

建设，可以实现针对智慧车站运营管控平台安全建设的复制推广。

政策合规：为运营管控平台提供信息安全保障的同时，使运营管控平台信息安全满足政策合规性，达到等保二级防护水平。

1.1.5 单位基本信息

北京六方云信息技术有限公司是一家技术领先的“新安全”公司，六方云借助人工智能技术仿生人体免疫机制，针对工业客户和政企客户的安全需求，创造性地提出了“AI 基因、威胁免疫”的“新时代、新安全”安全理念，采用+AI 和 AI+战略，将人工智能技术应用于全系列产品，构建安全威胁免疫系统。在国家新基建战略下，致力于提供关键信息基础设施保护、工业互联网安全的产品和解决方案，拥有保护工业客户和政企客户的“5+1”产品线：工控安全产品线、网络安全产品线、云安全产品线、安全态势感知产品线、人工智能安全产品线及安全服务。

六方云董事长任增强表示：工业互联网安全、云安全、人工智能安全是“新安全”，是未来，而未来世界发展的主要推动力来自于技术。六方云坚持以吸引和团结有共同价值观的人才为核心，持续不断地耕耘攻坚，实现“以技术保障技术”，用最先进的技术解决国家与行业在高速发展中的安全问题，保障国家工业互联网战略、云安全战略、以及新基建安全的实现，让万物安全互联。