工业互联网产业联盟
Alliance of Industrial Internet

工 业 互 联 网 产 业 联 盟 标 准

AII/022-2021

城市轨道交通工业互联网 信息管控系统 应用指南

Guideline for Industrial Internet information management and control systems of urban rail transport

工业互联网产业联盟

（2021 年 12 月 30 日发布）

目　　次

工业互联网产业联盟
Alliance of Industrial Internet

前　言

本文件按照GB/T1.1-2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由工业互联网联盟城市轨道交通特设组提出。

本文件由工业互联网产业联盟标准组归口。

标准牵头单位：上海宝信软件股份有限公司，成都轨道交通集团有限公司，上海申通地铁集团有限公司，广州地铁设计研究院股份有限公司，北京东土科技股份有限公司，北京启明星辰信息安全技术有限公司

标准起草单位和主要起草人：

上海申通地铁集团有限公司 姚湘静、朱钡伦
上海申通轨道交通研究咨询有限公司 洪翔
上海宝信软件股份有限公司 丛力群、崔岩、胡彦、葛鑫、安笑言
广州地铁设计研究院股份有限公司 毛宇丰
广州新科佳都科技有限公司 贾建平、陈朝晖、刘志宏
长扬科技（北京）有限公司 赵华
北京东土科技股份有限公司 闫志伟、李沁龙
北京轨道交通建设管理有限公司 王道敏、王颖、陈洪茹
北京启明星辰信息安全技术有限公司 赵军凯、谷宝晶
北京和利时系统工程有限公司 朱毅明、熊辉、宋小莉、刘小树
北京惠而特科技有限公司 谭曙光
西安市轨道交通集团有限公司 侯久望、王永州
成都轨道交通集团有限公司 黄嘉、赵雪
华为技术有限公司 宋军、陈伟玮、胡双
全国自动化系统与集成标准技术委员会 魏晓东
青岛海信网络科技股份有限公司 万思军、孙鹏飞、曹顶法
杭州迅维智能科技有限公司 卜凡起、姜凌青
杭州迪普科技股份有限公司 宋文刚
国电南瑞科技股份有限公司 许超、李潇潇、张浩、王硕
南宁轨道交通集团有限公司 黄俪、李梦和
南昌轨道交通集团有限公司 付胜华、陈星
南京轨道交通系统工程有限公司 邓敏、赵明桂
株洲中车时代电气股份有限公司 戴云陶
浙江浙大中控信息技术股份有限公司 王心光
深圳市赛为智能股份有限公司 赵健
湖南中大检测技术集团有限公司 张何猛、郭棋武
摩莎科技（上海）有限公司 王自胜、刘冬冬

工业互联网产业联盟
Alliance of Industrial Internet

引　言

当前，以新一代信息技术为驱动的数字浪潮正深刻重塑经济社会的各个领域，推动着生产方式、产品形态、商业模式、产业组织和国际格局的深刻变革，并加快了第四次工业革命的孕育与发展。而工业互联网是实现这一数智化转型的关键路径，是构筑第四次工业革命的发展基石。

城市轨道交通由线网指挥中心、线路控制中心、列车、车站、线路区间、车辆维修基地、主变电所等组成,业务范围涵盖设计、建设、运营、运维及企业管理、生态协同等方面。国内城市轨道交通普遍采用线网指挥中心、线路控制中心和车站综合控制室三级运营监控、调度指挥、运营维修及运营管理模式。

智慧城市轨道交通实施方案总体思路是紧密结合线网、线路和车站各级运营工作流程和实际功能需求，以既有自动化系统为基础，运用工业互联网技术，适当增设软硬件设备，对各类数据进行梳理和综合利用，实现数据支撑与技术支撑；建立具备场景化、智能化、人性化的智慧城市轨道交通综合运管平台，提供更多的应用模式和运营模式，实现更加全面、智能的管家式一体化应用功能，提高线网、线路和车站的运管效率，提升安全和服务水平，最终实现减员、增效、降本。

工业互联网产业联盟城市轨道交通特设组基于工业互联网技术架构体系，结合城轨业务特点,编制和发布《城市轨道交通工业互联网 信息管控系统 应用指南》，以网络、平台和安全三个功能架构层次为主线，以云边端三个实施层次为子线，定义了城市轨道交通工业互联网的体系架构，普及城市轨道交通工业互联网知识，凝聚用户、设计和产业界共识,为城轨行业的数智化发展实践提供科学、清晰和可操作的指南。

工业互联网产业联盟
Alliance of Industrial Internet

城市轨道交通工业互联网 信息管控系统 应用指南

1 范围

本文件规定了城市轨道交通工业互联网信息管控系统的体系架构。

本文件适用于地铁、轻轨、单轨、磁浮、市域或城际快轨交通、有轨电车等城市轨道交通领域,指导该行业采用工业互联网体系架构开展信息管控系统的设计开发和实施应用工作。

本文件依据《中国城市轨道交通智慧城轨发展纲要》智慧城轨建设要求，重点围绕城市轨道交通工业互联网体系架构的设备层、边缘层和企业层展开。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB-T 50833-2012 城市轨道交通工程基本术语标准

GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求

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-总体需求》

T/CAMET 11001.2-2019《智慧城市轨道交通信息技术架构及网络安全规范-技术架构》

T/CAMET 11001.3-2019《智慧城市轨道交通信息技术架构及网络安全规范-网络安全》

IEC61375 铁路电子设备 - 列车通讯网络

EN45545-2 铁路应用-轨道车辆防火保护 - 材料和元件的防火要求

EN50121-4 铁路应用-电磁兼容性 - 信号及通讯装置的发射及抗扰度

EN50155 铁路应用 - 机车车辆电子装置

工业互联网产业联盟
Alliance of Industrial Internet

3 术语和定义

下列术语和定义适用于本文件。

3.1

城市轨道交通信息管控系统 Information management and control system

城市轨道交通运营企业的信息业务包括运营管理、运维管理、企业管理、建设管理和行业协同管理，统称为信息管控系统。

4 符号和缩略语

5G	第五代移动通信技术
AFC	轨道交通自动售检票系统
API	应用程序编程接口
APP	移动应用
APT	高级可持续威胁攻击
BAS	环境与设备监控系统
BIM	建筑信息模型

CBTC	基于通信的列车控制系统
CCTV	轨道交通视频监控系统
DevOps	一种重视开发和运维间沟通合作的文化、运动或惯例
DOS/DDos	拒绝服务攻击
FTP	文件传输协议
GIS	地理信息系统
IP	网际互连协议
IPv6	互联网协议第六版
ISCS	城市轨道交通综合监控系统
LTE-M	城市轨道交通车地综合通信系统
MAC	媒体存取控制位址
Mail	电子邮件
Modbus	一种串行通信协议
NAT	网络地址转换
NFV	网络功能虚拟化
OPC	用于过程控制的OLE工业标准
PaaS	平台即服务
PIS	轨道交通乘客信息系统
Rlogin	远程登录
SDK	软件开发工具包
SDN	软件定义网络
SNMPV3	简单网络管理协议第三版
SRv6	基于IPv6转发平面的段路由
TCMS	列车控制与管理系统
Telnet	一种Internet远程登录服务的标准协议和主要方式
TOD	一种以公共交通为导向的开发规划设计方式
TSN	时间敏感网络
USB	通用串行总线
Web	万维网
WLAN	无线局域网

工业互联网产业联盟 Alliance of Industrial Internet

5 体系架构

5.1 功能架构

5.1.1 城市轨道交通工业互联网功能架构由网络、平台、安全组成，网络是基础，平台是核心，安全是保障。

5.1.2 网络构建生产网、管理网和服务网，将自动化与信息化融合，支持运营、运维、管理和协同数据的互通共享。

5.1.3 平台包括智能现场设备、边缘计算平台、信息管控平台和智慧城轨平台，是城市轨道交通全要素、全产业链、全价值链连接的技术支撑。

5.1.4 安全根据总体安全需求，开展对应安全架构设计，采取针对性安全措施，确保系统安全的持续有效。

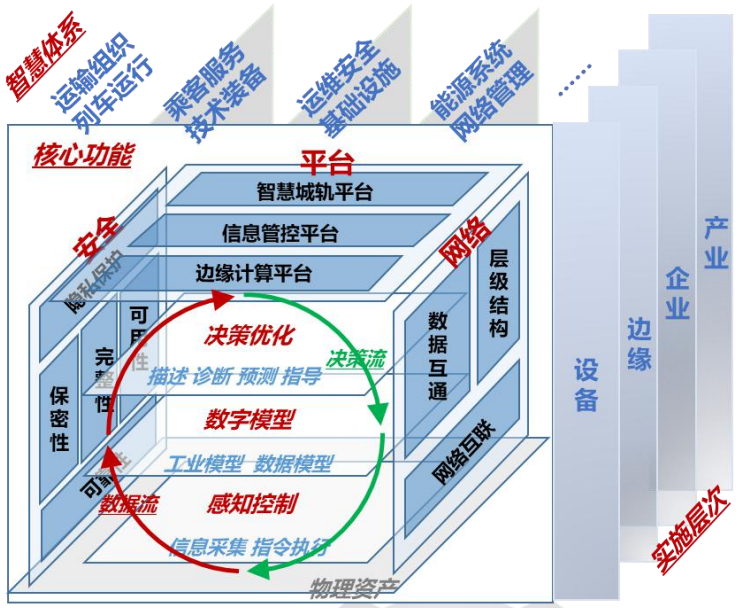

图 1　功能架构图

5.2　实施架构

5.2.1　城市轨道交通工业互联网的实施架构包括设备层、边缘层、企业层和行业层。各层次的数据在功能架构上贯通一体，共同支撑城市轨道交通八大智慧体系。

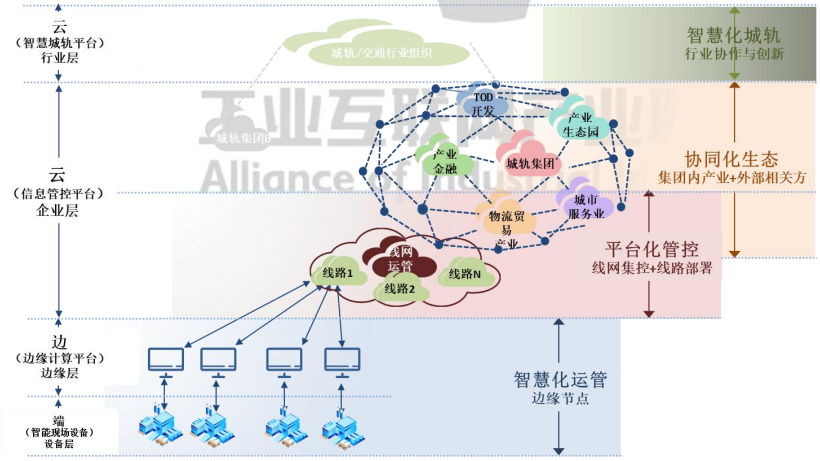

图 2　实施架构图

5.2.2　设备层由车站、车辆、车辆段、停车场的众多自动化专业设备组成，通过工业物联网连接在一起。工业物联网是城市轨道交通工业互联网的基础部分。

5.2.3　边缘层靠近物或数据源头的设备，是采用网络、计算、存储、应用为一体的开放平台，提供近端服务，满足现场的实时业务、应用智能、安全、高可用和降级运行等方面的需求。该层构建于工业物联网，由车站综合监控平台升级演进发展成为智慧车站边缘计算平台。

5.2.4　企业层由线路线网运营管理、运维管理、企业管理、建设管理和协同生态等应用系统构成，是城市轨道交通工业互联网的核心。该层宜构建于云平台和数据中心上，并最终升

级演进发展成为城轨企业的信息管控平台。

5.2.5 行业层由城轨或交通行业组织牵头构建，是城市轨道交通工业互联网的顶层应用系统，实现智慧城轨行业业务。

5.3 实施模式

5.3.1 城市轨道交通工业互联网的实施应充分考虑企业已拥有大量存量资产，可分为叠加和融合两种模式。

5.3.2 既有系统实施宜采用叠加模式。该模式是企业在原有系统之外，按照工业互联网的架构做新的部署，对现场数据类型和数据协议进行梳理、归类并建立标准，配置边缘计算软硬件环境，定义边缘计算相关功能，在云端中心积累微构件，进行模型化、组件化开发，并建设数据中心，在全新的架构下开发数据应用，将数据应用和企业原有系统叠加，再逐步对企业原有应用系统进行重构，慢慢将企业原有应用迁移至新的工业互联网平台中。

5.3.3 新建系统实施应采用融合模式。该模式是基于平台实现企业所有业务系统的部署运行，充分发挥平台数据管理、建模分析和应用创新优势，高效灵活地满足企业所有智能化需求。该模式实施的系统，现场数据统一由边缘计算平台进行采集和预处理，基于边缘计算平台开发面向智慧车站的管控系统;信息管控平台汇集全域数据,基于一体化平台开发全局型、协同共享型和通用型等应用。

5.4 实施重点

5.4.1 城市轨道交通工业互联网建设实施应“以数据为中心”。这是工业互联网区别于传统信息化的重点之一，“以数据为中心”有助于企业系统建设思路转变，更好地解决系统发展优化的问题。

5.4.2 城轨企业应逐步从“以流程为中心”的设计模式，转向“以数据为中心”的设计模式，更加关注数据与模型在业务功能实现中的分层演进作用，以达成更智能、更敏捷、更协同、更灵活的发展要求。

Alliance of Industrial Internet

5.4.3 城轨企业基于工业互联网，以构建数智化转型中的运营和发展优势作为其愿景，可从增进安全、创新模式、提升价值和降低成本四大战略方向进行努力。

6 业务功能

6.1 业务概述

6.1.1 城轨企业的业务系统可分为运营管理、运维管理、企业管理、建设管理、协同生态和行业业务，业务系统间相互协同支撑，互为数据供给方和消费方。

6.1.2 基于工业互联网架构，在安全保障（安全）下提高各业务系统的共融互通（网络），实现业务融合（平台），驱动轨道交通数智化转型。

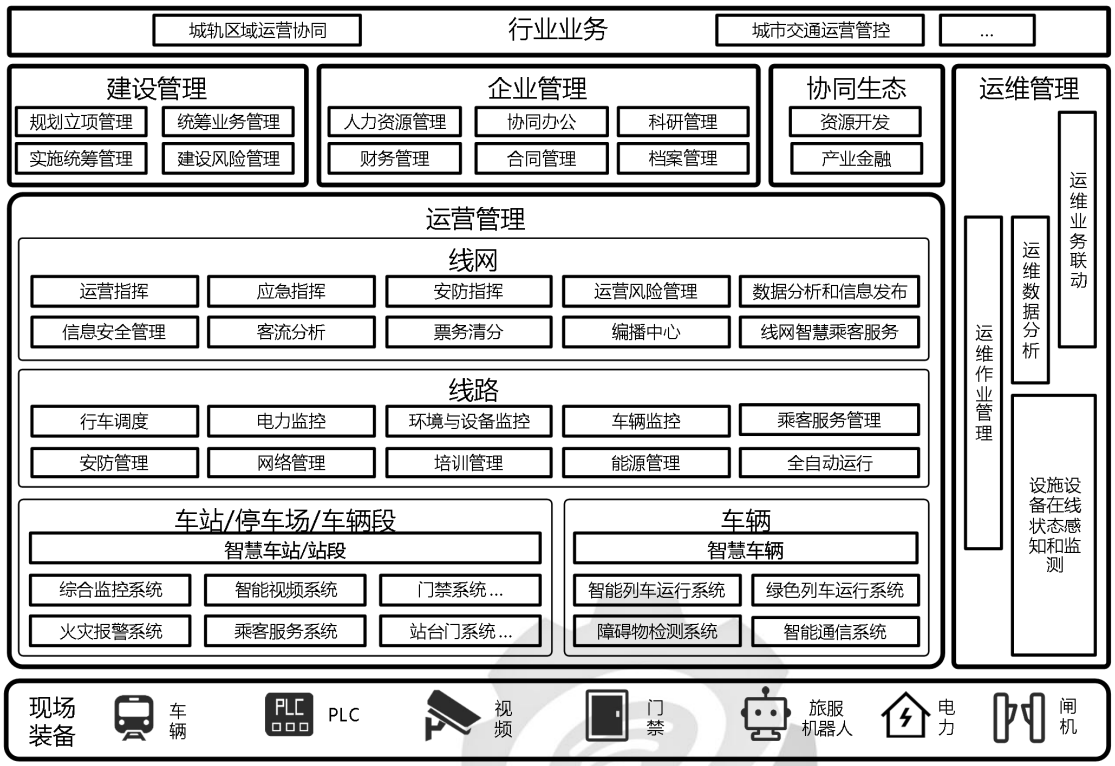

图 3　城市轨道交通业务功能图

6.2　站段功能

6.2.1　车站运营管理应由多个专业化信息管控子系统以及集成/互联这些子系统的综合监控系统平台所构成。新一代的车站运营管理体系应增加全息的物联感知能力，形成新一代车站级工业互联网边缘计算平台，赋能更加智慧化的乘客服务、设备管控、客运管理和站务管理，从而演进成为智慧车站。

工业互联网产业联盟
Alliance of Industrial Internet

6.2.2　车站级综合监控系统及其互联集成子系统聚焦于实时控制，针对智慧车站工业互联网边缘计算平台对全面过程数据的需求，应构建更加全面的运行工况全息感知体系，宜基于当前成熟可靠的物联网技术构建。

6.2.3　环境与设备工况感知应实现对环境参数和机电设备运行状态数据的全息感知。

6.2.4　智能视频应采用智能视频分析技术，提供站厅、站台、出入口、换乘通道等重要区域的客流状态以及异常行为告警。

6.2.5　站台门感知应实时采集站台门全息工况数据，宜具备远程控制功能。

6.2.6　门禁感知应在通道门处设置生物识别设备，实现对人员进出的感知与管理；宜与智能视频技术结合，实现巡检轨迹的感知记录。

6.2.7　火灾报警感知应更加全面地实时感知火灾报警系统的运行状态，包括报警内容及其位置信息；应分类存储统设备的运行、故障和报警的感知数据。

6.2.8　乘客服务系统增强宜与广播系统配合在站台门和自动扶梯处实现定向广播功能；自动扶梯、换乘通道等位置的乘客信息显示屏应显示车站信息、车站拥挤度、换乘等信息；站台的乘客信息显示屏应显示到站列车信息、车厢满载率、车站拥挤度等信息；车站出入口的

乘客信息显示屏应显示车站运营服务信息等；宜实现场景化乘客信息服务，根据乘客信息显示屏的位置和场景需求，能够个性化播放相关区域内容。应具备对自动售检票系统终端设备的远程控制功能，应具备移动支付购票或充值的功能，宜支持语音购票。

6.2.9　智慧车站应紧密结合车站级各运营班组的工作流程和实际需求，在既有控制及其互联集成子系统的基础上，增设全息感知物联网设备，构建车站级工业互联网边缘计算平台。

——智慧车站边缘计算平台应具备车站基本运作功能，包括但不限于数据库管理功能、输入数据处理功能、模式控制功能、顺控及点控功能、自诊断功能、时钟同步功能、监视功能、控制与调节功能、参数设置功能、事件回放功能、运营数据统计和决策支持功能、权限管理功能、内部运算功能、实时趋势与历史趋势记录功能、报警与事件管理功能、统计和报表功能、打印管理功能、历史数据存档和查询功能、组态维护功能和系统的备份与恢复功能等。

——智慧车站边缘计算平台应对各类数据进行梳理和综合再利用，建立起具备场景化、智能化、智慧化的车站信息管控功能，全面提升车站在乘客服务、设备管控、客运管理和站务管理等方面的能力。

——智慧车站应具备乘客服务功能，应采用智慧导乘系统、智慧安检、智慧客服、智慧厕所等技术为乘客提供更快捷更优质的服务。

——智慧车站应具备设备管控功能，应实现设备的智能监控、智能诊断、智能巡视和故障报修管理；通过综合电能、节能运行模式数据对车站运行耗能进行智能分析，实现车站的能耗管理；通过环境智能感知设备，实时感知车站环境，实现车站环境的智能化管理。

——智慧车站应具备智能巡检功能，可基于统一的 BIM 可视化系统对车站关键系统的设备进行模拟一键点巡检，辅以适当的视频分析技术，实现替代人工现场巡检的工作，提升日常巡检效率。应能对当前运行状态进行采集、归类、汇总，提供各系统专业设备一键可选择性查询，支持自定义专业设备巡检，并对巡检结果进行归纳，统计和对比，为车站设备报修、巡检提供数据支持。

——智慧车站应具备设备管家功能，应实现基于既有 ISCS、BAS 系统与风机、水泵、站台门、电扶梯等机电设备接口，通过增加传感器、水流指示器（选用）、压力传感器（选用）、在线检测装置等，从车站、区间等大型设备就地采集状态参数，通过分析、处理来实现对设备的实时监控、故障预警。设备管家应至少实现维修支持功能、综合智能分析功能和三维可视化管理功能。

——智慧车站应具备环境在线监控功能，应实现车站设备及运行环境信息的集中管理，对设备运行环境状态进行综合诊断，更及时、准确、灵敏地反映设备及运行环境的当前状态。智慧车站环境在线监控采集点应至少包括公共区域环境、出入口环境、新风井环境和机房环境。智慧车站应结合环境检测报警或异常数据，针对站内空调冷气排放、阀体、大小系统、排热风机等设备实现实时控制，以便改善车站环境质量、提高乘客体验舒适度。

——智慧车站应具备消防监测功能，实现对消防关键系统设备监控功能，并对异常情况实时提示。

——智慧车站应具备车站消防演练功能，当建筑消防分区发生火灾时，展示系统联动设备状态、着火位置现场图像、疏散指示标识、广播提醒和操作卡提示等信息，供车站人员日常消防演练和培训使用。

——智慧车站应具备节能功能，并通过综合电能、水量及节能运行模式数据，将车站运行耗能送给线路能源管理系统。

——智慧车站应具备客运管理功能，通过构建车站人员定位、人脸识别门禁、智能视频巡视等系统，结合业务系统中人、事、物及其关联的数据和信息，展现车站值守、巡视、客运和服务等各项工作效能，实现对车站人员的全方位管理。

——智慧车站应具备车站多专业系统联动能力、应急处置能力和应急演练能力。在突发应急事件（如：突发大客流等）情况下，能自动启动相应的处置预案，联动相关设备按照预定方式运转，降低车站工作人员人工监视、判断和处置的工作量。

——智慧车站应具备智能开关站功能。智能开关站包括设备状态自检、人工视频确认、开关站操作执行、保存历史等步骤。智慧车站应采用智能化的手段保证开/关站的可靠性和安全性。

——智慧车站应具备客流管理功能，应在车站公共区设置嗅探设备，通过无线和有线传输方式将该数据传递给智慧车站，通过结合进出站客流、智能视频分析客流密度等信息，经人工智能处理后，形成车站客流密度及流向分析数据，实现客流分布展示及越限报警，为下一步的运营客运组织和管理提供有效的数据支撑。

——智慧车站应具备智能视频联动功能，应基于智能视频提供的分析结果，实现客流状态、乘客行为异常、设备故障、开关站辅助等动态检测，并能触发自动联动功能。

——智慧车站应具备站务管理功能，通过施工调度系统、站务系统等接口系统，全面了解车站的施工管理信息，排班布岗信息，设备巡检信息等，实现站务信息的综合管理。

——智慧车站应具备人员管理功能，应利用门禁监控、视频监控、人员定位等功能，通过生物识别身份认证、黑名单等技术，实现车站工作人员管理、车站人员（含施工及委外人员等）进出权限管理和巡更管理等人员管理。

——智慧车站应具备智能排班功能，应为车站值班人员提供日常排班功能，运营人员可根据车站值班规则自主定义车站轮班，根据录入的排班规则自动生成值班表，支持运营人员自主修改值班表功能。

——智慧车站宜建设全息感知物联网，监视管辖范围内供电、信号、车辆等关键设施设备的状态。

工业互联网产业联盟
Alliance of Industrial Internet

6.3 车辆功能

6.3.1 车辆应实现智能列车运行系统及装备。该系统及装置适用于全自动运行，可实现不同制式的轨道交通信号系统互联互通、车辆匹配，提升线路运能，降低系统能耗，支持“四网融合”。该系统及装置通过引入人工智能技术，提升列车智能水平、优化列车驾驶性能和适应性；采用新一代车地通信及环境感知系统，加强列车对于行车空间及车上空间的信息感知能力；实现列车协同最优控制，提升运行效率和运营灵活度。

6.3.2 车辆应实现车辆智能通信功能。车辆智能通信推进非行车安全信息车地通信向5G+融合演进，推动5G+技术在城轨行业应用落地，实现开发超大容量、全分布式组网、智能流量分配的新一代有线承载网络；实现集语音、图像、数据等多媒体信息为一体的新型智能多媒体调度系统；强化智能通信信息安全，确保通信业务和数据资源的机密性、安全性和完整。基于成熟技术体系进行系统核心功能智能融合、协同控制，打破信息壁垒，融合智能控制、智能感知、智能诊断，实现从分离系统多节点控制转变向集中“控制、诊断、思考与决策”转变，构建智能、安全、可靠、多元的多系统融合方案，实现技术装备智能化、智慧化。

6.3.3 车辆应实现高效绿色列车运行系统及装备。该系统及装置基于优化城轨能源系统设计的理论方法，通过分析能耗-客流的耦合关系，充分利用客流、车辆、信号、环境控制等综合信息建立能源系统动态模型，并探索直接使用市电系统供电的方案，实现线网级能源调

度、优化行车组织、编制节能运营图等功能，实现总体对城轨运营节能效率的提升。

6.3.4 车辆应实现可靠安全的障碍物检测系统及装备。该系统及装备用以解决城市轨道交通运营过程中非预期的障碍物对行车安全带来的不利影响，降低人工瞭望与巡检工作强度，提升运营安全水平。对于城市轨道交通碰撞的检测，目前主要采用被动防撞探测杆，通过被动防撞探测杆碰撞到障碍物目标后，引发列车紧急制动，从而降低碰撞损失。随着先进感知和边缘计算技术的发展，光学检测、激光雷达、毫米波等传感器技术、人工智能技术和边缘计算能力的不断提升,在车载端通过传感器提前感知行车前方障碍物信息,将其转换为图像、点云、电磁波强度等数字信号，在边缘平台通过人工智能算法进行处理后，识别出障碍物的类型、坐标、速度等信息，预测碰撞风险，与车辆控制系统联动，引导列车完成主动防撞动作。

6.4 线路功能

6.4.1 城市轨道交通线路功能应实现线路整体的行车调度、电力监控、环境与设备监控、车辆监控、安防监控、乘客服务管理、网络管理、培训管理、能源管理、全自动运行等功能，管理的范围包括线路中心/备用中心、车站、车辆段、停车场、主变电站、集中冷站、车辆、轨道、通信网络等设施和系统。

6.4.2 行车调度应实现对全线列车运行的自动管理和监控，主要包括时刻表编制与管理、当日运行计划管理、列车运行计划与管理、列车跟踪与识别、自动排列进路、调整列车运行等功能。

6.4.3 电力监控功能包括电力调度、设备监控、智能程控管理、智能报警决策、供电智能巡检、调度命令电子化等功能。

——电力调度采用“统一调度、分级管理”的原则，保证全线路供电系统安全、可靠运行和连续供电；保证供电的电能质量、负荷分配符合规定标准；使供电系统在经济和合理的方式下运行。

——电力设备监控应实现对全线电力设备的状态监视、单遥控制、顺序控制、数据分析处理、远程运行维护、统计报表、事故报警等功能。

——智能程控管理应以列车运行图、检修计划、设备故障跳闸等作为输入条件，通过预设程控卡片，实现对供电系统的自动停送电及倒闸操作。同时自动联动广播系统、变电所智能巡检系统给与辅助支持。

——智能报警决策应实现故障智能研判分析、推荐紧急控制策略、提供调度辅助决策、实现供电系统自愈与重构、基于多种数据来源的电力故障分析及应用。

——供电智能巡检应按照检修计划自动调用设备数据和相应的摄像头视频,实现全线牵引供电系统的巡视。

——调度命令电子化应通过调度命令的新建、编辑、审核、下发、签收等功能，实现调度运行管理的电子化和表票的自动化流转。

6.4.4 环境与设备监控应实现对全线路机电设备状态的监视、设备报警的管理，通过模式控制、时间表控制等功能实现自动控制设备运行，检测环境参数，调控环境舒适度及节能管理。确保设备处于安全、可靠、高效、节能的最佳运行状态，从而提供一个舒适的乘车环境。

6.4.5 车辆监控应实现监视车辆上各个子系统的主要设备运行状态、报警信息等，对车辆设备进行初始化控制和远程控制，组织指挥对车辆上设备的维修工作等。

6.4.6 乘客服务管理应实现全线 PIS 控制器状态、广播设备状态监视，编辑发送 PIS 屏播

放文本，实现按照广播区广播、预录广播等；应监视全线所有在线运行车辆中车载视频监控、广播、应急对讲、乘客信息等乘客服务设施状态，远程监控车辆照明及空调系统；接听车辆上乘客应急语音对讲电话，并通过车载视频监视车内情况。

6.4.7　安防监控应实现站段、主变电所等设备和管理用房、出入口、票务室等重点区域的出入管理、登记、实时视频监控等功能，实现事件的实时传达、告知、报警，以使事件能够在最短的时间内得到处理和备案，有效保障城市轨道交通运营安全。

6.4.8　网络管理应能监控系统主要设备的运行状态，实现系统设备在线自诊断和故障定位功能，实现对网络设备进行配置管理、参数管理、状态查询等功能。

6.4.9　培训管理应在培训环境中对生产系统进行全方位信息模拟，包括电力监控系统、环境与设备监控系统、广播系统、乘客信息系统等，便于学员操作学习；可将生产系统中数据在培训环境中进行回放，便于对实际工况的掌握；提供考试系统便于对学员所学技能知识进行考核。

6.4.10　能源管理应实现对全线电能、水、燃气等能耗的实时监测、历史记录、趋势显示、自动抄收、查询统计、数据分析、能耗质量分析、能效对比分析、报表功能等功能。

6.4.11　全自动运行应实现自动牵引上电、自动唤醒列车、列车自动出库、正线自动调整、列车自动回库、列车自动休眠、自动洗车等功能；应实现列车脱轨/障碍物相撞监测、站台门间隙探测防护等功能；应实现全自动运行中故障的自动处理，主要包括：车门故障隔离站台门、站台门故障隔离车门、列车驾驶模式转换、列车故障复位、列车故障旁路等；应实现中心应答乘客呼叫、列车雨雪模式运行、列车遇障碍物处理、火灾情况处理、区间自动疏散等应急自动处置功能。

6.5　线网功能

6.5.1　城市轨道交通线网功能涵盖网络级运营指挥、应急指挥、安防指挥、运营风险管理、信息安全管理、数据分析和信息发布、票务清算管理、客流分析决策、智慧乘客服务、编播中心等功能。

Alliance of Industrial Internet

6.5.2　运营指挥应实现对线网行车、客流、设备运行、故障、灾害预警等进行不间断监视；线网运行图编制与监督，以及线网客流和运输组织的匹配；线路换乘衔接和跨线路运营协调指挥。

6.5.3　应急指挥应实现线网应急预案管理与演练；应急情况下跨线路的运营组织协调，跨单位的应急物资及应急力量协调。

6.5.4　安防指挥应实现统一管理各线路技防系统，实现公共安全可视化、系统联动一体化和应急指挥科学化，以提升轨道交通工程防控能力，降低城市轨道交通区域内发生安全威胁的可能性。

6.5.5　运营风险管理应实现线网运营风险的分类、采集、管理、分析和预警管理，为线网运营风险控制提供决策辅助支撑。

6.5.6　信息安全管理应根据信息系统安全等级保护三级的规定，综合考虑物理层面、网络层面、系统层面、应用层面和管理层面的安全需求，确保线网指挥调度系统安全稳定运营

6.5.7　数据分析和信息发布应实现运营生产指标计算、分析、管理、评估；对企业内报送运营信息、编发运营报表；实现对企业外发布运营信息，包括官网、官方手机应用、微博、

微信及其他面向乘客服务的载体；实现应急情况下向更高一级企业应急管理机构报送信息。

6.5.8 线网票务清算管理应实现各线路统一制定、发行和管理轨道交通联网专用票（一票通）；具备多元化支付平台功能，承担轨道交通非现金支付中心作用。

6.5.9 线网客流分析决策应实现利用客流数据和行车数据进行深度分析，实现客流的分时段预测、异常情况下客流重构分析等功能，强化票务管理及服务营销分析，为线网运营管理提供全方位决策辅助。

6.5.10 线网智慧乘客服务应通过人性化、智能化的服务手段，实现智能客服、多元票务、服务质量监控、自适应诱导等功能，实现对乘客出行全过程服务需求的主动感知，围绕资讯、出行等关键服务内容进行智能整合、构建新时代智慧出行服务体系。

6.5.11 线网编播中心应在具备集中监播、节目编辑、下发等线路编播室功能前提下，为各线路乘客信息服务系统提供统一的信息源、管理模式及营销渠道，实现多运营主体情况下的编播控制。

6.6 运维功能

6.6.1 城市轨道交通运维功能应以设备设施、规程为基础，依据维修维护作业的组织策划和检修计划管理，落实计划修、故障修、状态修等维修模式的管理要求。系统功能包括：设施设备在线状态感知和监测、运维作业管理、运维数据分析、运维业务联动等功能。

6.6.2 城市轨道交通运维功能应满足不同专业设备设施运维功能的共性和个性化需求，专业分类包括但不限于：基础结构类、行车运输类、乘客服务类、车站设备类等专业分类。

6.6.3 设施设备在线状态感知和监测应按设备层次结构，建立设备设施信息库。设备设施信息包括：建筑、部门、设备布局、基本技术参数、采购信息、运行过程中的实时故障/健康状态、维修记录等，并对设备增加、调拨、位置变更、技术状态变更等动态信息提供台账记录和查询功能。

工业互联网产业联盟
Alliance of Industrial Internet

6.6.4 运维作业管理应以可靠性为核心，以减少关键设备故障维修概率、优化预测性维护相关标准为目标导向，功能包括：巡检作业管理、维修作业管理、设备履历管理、故障管理、工单管理、人员管理、物料管理等。

——巡检作业管理：包括创建巡/点检计划安排，记录巡/点检结果，生成巡/点检报表以及统计巡/点检完成情况、问题等工作。
——维修作业管理：根据设备履历定修要求、或故障录入确认、或设备设施状态监测，触发创建维修及保养工单。工单任务完成以后，应生成维修报告，并对评估运维人员工作效率及质量。
——设备履历管理：主要对设备信息进行维护管理，包括设备台账管理、备品备件管理、工作票管理、修志修程管理等。
——工单管理：实现对工单的登记、派工、提醒、受理、完工、评估、综合查询、报表等全生命周期过程进行管理和统计分析，支持设备树的快速查询，支持分层分级的工单传送。
——人员管理：实现人员基本信息登记、组织架构管理，实现排班、调班、考勤管理，实现多维度的数据统计分析及人员考核。
——物料管理：实现对维修所需的备品备件、工具设备等统一管理。

6.6.5 运维数据分析应基于大数据建模技术对设备设施的运维数据进行分析，发现长期性

的、规模性的、多维度的设备运行规律，为设备设施在线监测、维修处置建议、运维流程优化以及设备保养、备件采购、库存决策、人员培训、设备运行优化等业务提供建议。运维数据分析模型包括：设备机理模型、运维场景模型、统计分析模型、人工智能模型等。

6.6.6　运维业务联动应基于大数据的运维管理体系顶层设计，通过对全生命周期（建设、运营、管理）运维业务数据的积累和管控，建立“设备、人员、技术、管理”四位一体的城轨线网运维生态服务体系和运营维保支撑体系，实现企业资产管理、采购管理、仓储管理、供应链管理等业务的数据赋能。

6.7　企管功能

6.7.1　轨道交通企业管理承载集团和下属单位、部门的各种企业管理相关业务，为建设管理业务、运营管理业务、维保管理业务等各业务板块提供基础支持。企业管理系统包括协同办公、人力资源管理、财务管理、合同管理等。

6.7.2　协同办公采用统一的平台和界面，以多屏方式展示运营、运维、建设、经营全流程的业务信息，满足企业不同层级、不同角色员工的日常办文、办会、业务事项处理、沟通和协作、学习和交流、信息查询和决策、个人事务办理、生活服务和社交等全方位需求。其组成包括以下部分：企业内部门户、企业移动门户、企业用户管理、企业工作流。

6.7.3　人力资源管理根据企业的战略发展要求及行业特点，实现企业选人、育人、用人、留人的全过程闭环管理。其功能主要包括：组织管理、人事管理、招聘管理、考勤管理、培训管理、员工绩效管理、薪资福利管理。

6.7.4　财务管理根据财经法规制度，按照财务管理的原则，组织企业财务活动，处理财务关系的一项经济管理工作，其功能主要包括：预算管理、费用控制管理、资产管理、财务核算管理、资产移交管理。

6.7.5　合同管理系统对企业所有类型的合同、合同全生命周期业务信息进行管理。系统功能主要包括：合同业务管理、合同台账、审计管理、法务管理等。

工业互联网产业联盟 Alliance of Industrial Internet

6.7.6　企管功能还包括党纪工团、科研管理、技术管理、档案管理、修志管理、信息服务、外事宣传等。

6.8　建管功能

6.8.1　轨道交通建设管理业务当前是轨道交通企业的核心业务之一，是运营管理和维保管理业务的基础，应涵盖规划立项管理、实施统筹管理、建设风险管理和集团统筹业务管理等业务。

6.8.2　规划立项管理主要承担网络优化、项目立项的工作，负责工程项目实施的前期统筹和管理工作。包括业务网络优化、项目立项、项目组合等。

6.8.3　实施统筹管理主要承担网络建设项目组合的设计管理、计划统筹、建造监管、验收管理、竣工移交和项目评估等重要功能，实现建设实施的项目组合与集中统筹管理。业务包括：计划统筹、建造监管、验收管理、项目评估；进度计划（多层级）、前期工程、建造实施、验收执行、竣工移交；资产编制、前期工程、实施进度、施工协调、验收整改等。

6.8.4　建设风险管理针对企业建设风险、项目交付风险、项目运营风险、安全与可建造性风险等各类风险建立治理机制，承担等级管理、风险监控、应急管理的功能，有效控制风险发生对一个或多个项目目标带来的负面影响。包括业务如下：等级管理、风险监控、应急管

理；质量安全，质安填报、事件管理、质安整改等。

6.8.5 集团统筹业务管理指建设管理板块中由企业管理平台提供的集团统筹业务，涉及企业管理业务多项功能，但更针对于建设项目维度来组织实施。业务包括：合约管理、信用管理、投资控制、预案管理、档案管理、知识管理、技术管理、绩效管理、标准管理；合约成本、档案标识、投资控制（多层级）、设计管理、绩效执行、知识管理（多层级）；接口协调、预归档管理等。

6.9 协同生态

6.9.1 协同生态主要包括资源开发、产业金融等方面。

6.9.2 资源开发围绕广告、商业、通信、物流等方面的提供资源基础信息和业务的管理，实现供应协同。具体广告、物流、贸易、产业园、TOD 开发等。

6.9.3 产业金融围绕城市轨道交通上下游产业链，实现融通资金、整合资源、价值增值，将产业与金融的紧密融合，在融合中加快城轨产业的发展。

7 网络要求

7.1 业务需求

7.1.1 城市轨道交通网络应考虑安全生产、内部管理、外部服务等业务应用接入需求；安全生产应满足传统线路综合监控系统、自动售检票系统、通信系统、乘客信息显示系统、安防系统等接入需求；支持接入不同业务系统的终端设备，实现对终端进行管理和调度，并对终端上传的数据进行管理。

7.1.2 针对智慧城轨新增智慧应用系统，网络宜支持智能车站类业务、智慧出行类业务、智慧运维类业务、智慧经营类业务等多种应用数据统一承载，宜根据业务需求和特点复用网络资源，避免网络重复建设。既有线改造时可考虑统一设置专网，避免影响运营线路生产业务正常运行。

工业互联网产业联盟 Alliance of Industrial Internet

7.1.3 城市轨道交通不同业务系统及应用在带宽、时延、可靠性、安全性等方面存在差异性，为匹配不同业务网络的融合承载，网络宜支持网络切片、时间敏感网络等技术，提供不同业务所需的连接服务和性能保障。

7.1.4 针对城轨云发展趋势，宜支持协同运维能力，支持自动化、智能化的综合智能运维能力；针对 LTE-M 和 5G 承载，应支持高精度时钟同步需求。

7.1.5 城轨云骨干网网络应采用冗余的网络架构，避免单点失效，保证网络的稳定运行。

7.2 网络架构

7.2.1 根据网络应用场景，智慧城轨的网络整体架构宜分为数据中心网络、线路线网骨干网、站段局域网、车地无线网络和车载网络五类网络。

7.2.2 数据中心网络应考虑业务云化演进需求。

——数据中心网络应采用云模式建设，采用模块式架构，标准核心交换机与接入交换机全连接组网，支持灵活扩展。

——数据中心网络应采用软件定义网络 SDN 技术和网络功能虚拟化 NFV 技术，实现端到端网络、安全和业务的协同，提供业务自动化开通部署和运维能力。当涉及业务迁移、业务上下线时，网络变化和安全策略自动协同，实现安全和网络同步部署的端到端防护，实现云平台、网络、安全联动控制、威胁联动处置。

7.2.3 线路线网骨干网按照技术类型可划分为传输骨干网和数据骨干网。

——传输骨干网宜采用光传送网或切片分组网技术承载。数据骨干网宜采用灵活以太网技术，实现车站边缘计算平台、业务 IP 终端和城轨云平台三层互联，数据交互。
——数据骨干网宜采用核心-汇聚-接入三层架构，采用线网云中心、集团总部等作为核心层，各线路中心或分公司总部作为汇聚层，车站、停车场等作为接入层。
——数据骨干网应考虑城市轨道交通数智化转型和业务云化演进，视频和协同办公等各类业务发展所产生的流量增加需求。宜支持根据网络流量变化，灵活调配负载或灵活调整自身拓扑和链路容量。网络设备应预留足够槽位数量，可以平滑扩容。

7.2.4 站段局域网应充分考虑边缘层物联业务需求。

——站段局域网宜增加生产无线网络覆盖，支持人员定位、热力采集、人员轨迹采集功能，并作为生产移动终端、移动客服设备无线传输通道。应对 WLAN 信道进行统一规划，保证信道之间不相互干扰实现无缝漫游，全覆盖，不掉线。
——站段局域网应考虑站段工业物联网融合，在不影响业务的前提下，宜采用融合方式组网，避免重复建设网络。网络建设应考虑不同系统间的隔离，避免故障范围扩大，需在站段局域网与线路骨干网、子系统间实现业务隔离。
——站段局域网设备应考虑轨道交通工业现场环境特殊性，设备应符合 EN50121-4 标准并满足宽温，防尘、高可靠等工业级要求。
——站段局域网建设应考虑系统对冗余的要求，AFC、CCTV、PIS 等需考虑链路冗余，并在关键节点实现设备冗余，CBTC、ISCS 等需要实现网络级冗余，采用双网架构。
——站段局域网建设应考虑目前及未来业务发展对网络带宽的需求，宜采用至少千兆带宽组网。
——站段局域网建设应考虑不同系统对数据传输延迟、抖动的需求，宜对不同类型的数据流分配相应优先级。
——站段局域网建设应考虑网络监控的要求，需使用网管设备组网，宜采用支持 SNMP V3 的设备实现安全管理。

7.2.5 车地无线网络应满足高带宽、低时延、快速漫游切换的应用需求，实现多业务综合承载，降低网络建设成本;亦应考虑无线网络安全防护，同时避免与民用无线网络系统的频段干扰。

7.2.6 车载网络建设应充分考虑以下设计需求。

——车载网络考虑列车震动、电磁干扰环境的特殊性，车载网络设备应满足 EN50155 及 EN45545-2 标准。
——车载网络建设宜考虑 CBTC、TCMS、PIS 融合，精简网络架构避免重复建设。同时应保证系统高可用性、高可靠性要求。
——车载网络建设时宜考虑下一代列车通讯网络规范 IEC61375 的要求，以满足未来网络通讯需求。
——车载网络建设时应统一规划网络地址，特殊情况网络设备需支持 NAT 功能以满足车地通讯要求。

Alliance of Industrial Internet

7.3 未来发展

7.3.1 城市轨道交通宜根据建设发展需求和阶段，选择自建专网，混合组网以及虚拟专网三种 5G 建设模式之一，进行试点探索。

7.3.2 未来车站工业物联网宜采用融合 TSN 网络，精简网络架构，降低网络建设成本及运维成本。

7.3.3 未来城轨网络宜支持 IPv6 和 SRv6 等协议栈。

8 平台要求

8.1 层次架构

8.1.1 城市轨道交通工业互联网平台采用 “云-边-端”分布式架构，由智慧城轨平台、信息管控平台、边缘计算平台和智能现场设备分别承载行业层、企业层、边缘层和设备层四个实施层次。

图 4 业务功能与实施框架关系图

8.1.2 平台应服务于业务功能，城市轨道交通工业互联网建设发展的重点为企业业务。

8.2 边缘计算平台

8.2.1 边缘计算平台承载了车站、站段和车辆等边缘层的业务，架构可分为基础设施层、数据接入层、数据存储层、数据处理层。业务应用层为基于该平台开发的应用集合。

8.2.2 叠加模式的边缘计算平台，各子系统的控制主机和前置采集器部署在独立的物理服务器或虚拟服务器上，与相连设备一起构成了典型的工业物联网。因各子系统数据存储和数据处理相互独立，数据互联一般通过接口相互调用，或部署独立的数据存储来解决；涉及数据融合运算，则各子系统内增加处理模块，或部署单独的数据处理系统来实现。

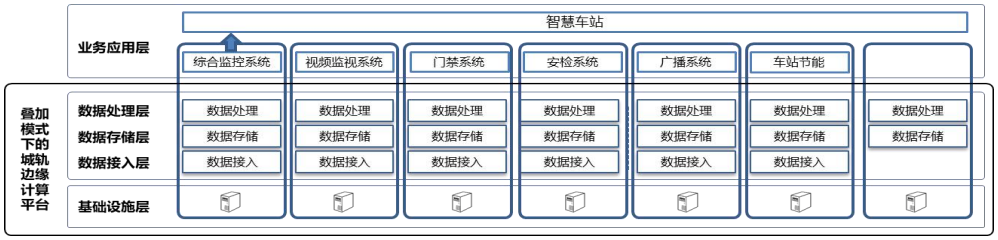

图 5　叠加模式边缘计算平台架构图

8.2.3　融合模式的边缘计算平台基于站段边缘计算节点，将接入、存储、处理的通用功能从各个业务应用系统中分离出来统一部署，实现基础设施和服务软件的高度融合。边缘计算平台统一的数据存储层实现了边缘侧的数据融合；统一的数据处理层提供的通用数据分析、基础算法、智能模型等功能；业务应用具备更好条件来开发更多智慧运营场景。

图 6　融合模式边缘计算平台架构图

8.2.4　综合监控系统和智慧车站管控系统的开发平台均具备融合模式边缘计算平台的特征。综合监控系统与其集成的子系统共用前置采集器和控制主机，通过集成或互联的方式，对大部分专业系统及其设备实现了数据的接入、处理、存储以及边缘层应用逻辑处理。智慧车站管控系统在综合监控基础上，进一步增加了车站节能和安防等系统的集成，以及车站的站务管理、客运管理和乘客服务等信息系统的融合。

8.2.5　融合模式边缘计算平台应提供通用功能包括：

——数据服务：信息管控平台的数据平台或其他外部系统对边缘数据的接入，包括应用状态监控、事件、报警等数据；
——组态工具：用以开发实时展示画面的低代码开发工具；
——平台管理/接口:边缘节点管理服务,且可实现信息管控平台的管理接入已满足统一管理要求，包括但不止：交付管理、运营管理、权限管理等；
——事件管理：边缘业务统一的事件管理中心；
——报警中心：边缘业务统一的报警服务中心；
——统一登录：登录验证系统以支撑降级作业，且可与信息管控平台同步权限以满足统一授权作业。

8.3　信息管控平台

8.3.1　信息管控平台承载了运营管理中的线路和线网业务，运维管理中的分析、管理和联动业务，以及企业管理、建设管理和协同生态的业务全部。其所含的信息系统的部署模式常采用“数据库服务器-应用服务器-客户端浏览器”架构；而运管系统则采用“接入层-存储层-处理层-客户端”架构。

8.3.2　叠加模式的信息管控平台，各个业务系统常采用独立的系统设备和数据，相互分割形成竖井。通过建设大数据中心，将各个业务系统的数据存储在一起，经过治理、建模、挖掘、可视化等步骤，将综合分析结果反馈给业务系统，实现高效智慧，在一定程度上解决数据融合的问题。

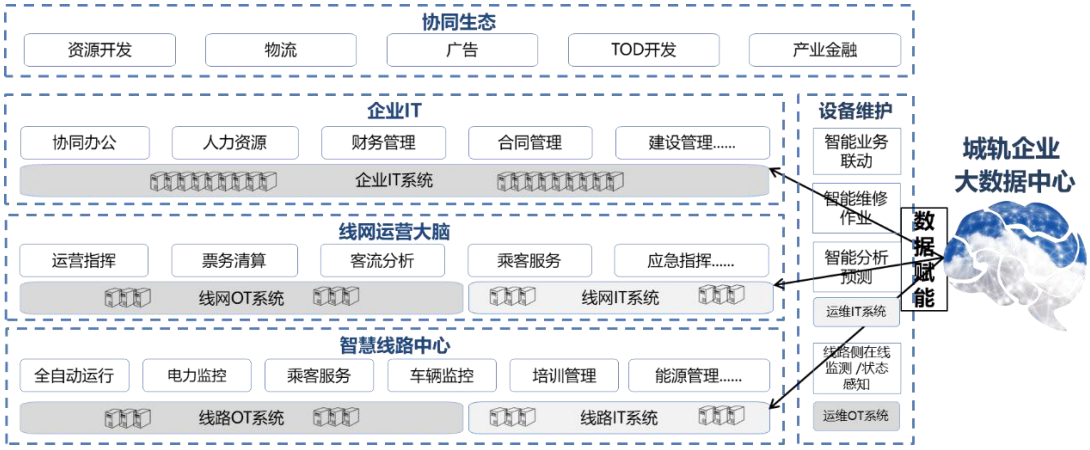

图 7　叠加模式信息管控平台架构图

8.3.3　信息管控平台宜采用云计算技术，将硬件资源的供应模式由传统竖井式转变为以资源共享的云服务方式，实现基础架构模块与业务模块松耦合、资源池的模块化交付和横向扩展，保证资源的快速交付和统一管理，支撑业务快速上线、融合运营、统一运维。

8.3.4　信息管控平台宜采用分布式、微服务、大数据、云计算等新一代信息技术，构建一个数字化、智能化、生态化的融合模式的信息管控平台，具备以泛在连接为基础、以平台使能为核心、以数字运营为支撑的三大特点，赋能城市轨道交通运营集团生态圈建设。

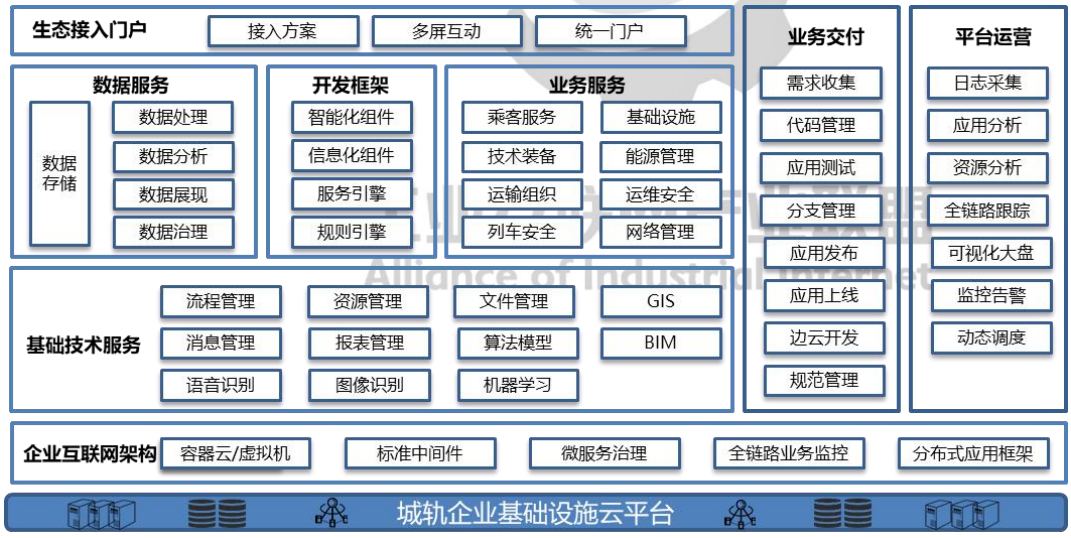

图 8　融合模式信息管控平台架构图

8.3.5　融合模式信息管控平台可提供的通用功能包括：

——生态圈标准接入门户。作为生态圈统一入口，负责圈内外用户间的信息传递。提供统一的应用接入门户的标准规范、工具和 SDK，以及跨平台智能生态 APP 移动应用的统一集成方案，用以发布内部应用信息，实现多屏幕、全方位、全业务的用户访问入口，提高用户体验。

——支撑应用敏捷迭代的开发框架。为项目开发团队提供一个完整的稳态及敏态 IT 架构和开发微服务架构所需的各种基础引擎服务、智能化/信息化界面组件等，帮助团队快速构建高可扩展、高性能、低成本的分布式系统，并做到底层技术、微服务架构、开发模式、数据交互标准全局统一。

——面向智慧城轨的业务服务。通过收敛、沉淀、标准定义，在服务注册、服务发现、服务编排的整体框架支撑下，形成满足城市轨道交通运营企业的乘客服务、基础设施、列车安全、技术装备、能源管理、网络管理、运输组织、运维安全八大智慧领域的业务组件，向合作伙伴和第三方提供数据和业务服务。

——贯穿全生命周期的数据服务。提供完善的数据服务能力，依托大数据技术，围绕数据全生命周期管理，贯穿数据接入、存储、处理、分析、展示的每个环节，提供专业的数据数字化、服务化、智能化、可视化、标准化的技术组件。

——完备的基础设施技术服务。提供完备的底层基础设施的技术支撑。主要包括信息资源管理、流程管理、文件管理、消息管理、报表服务、GIS、BIM，以及人工智能等功能组件。

——稳定高效的企业互联网架构。满足高可用、高性能、稳定性好等要求，为平台范围内的各类应用提供云计算基础、标准中间件服务、微服务治理、分布式应用框架、全链路业务监测等基础构件。基于高可用分布式 PaaS 服务来构建，以简化互联网架构应用的开发、运行和维护成本，为分布式应用提供一个完整的、高可用的平台服务能力。

——满足 DevOps 三级标准的业务交付平台。满足 DevOps 三级标准建设业务交付平台，实现需求收集、规范管理、代码管理、应用测试、分支管理、应用发布、应用上线等项目全生命周期管理的过程，并为单体应用和微服务应用提供开发框架支撑，对公共组件的复用进行统一管理，提供云边协同开发能力，支撑研发运营一体化。

——平台数字化生态运营。构建统一的集中管控中心，以数据化运营和穿透式运维为目标，对数据日志进行采集分析，服务数据分析，安全防护分析、全链路跟踪分析，提供可视化大盘，指标分析及监控告警等功能，实现统一的平台运营，满足动态调度、生态运营、共享系统等运营要求。

8.4 云边协同

8.4.1 城市轨道交通工业互联网平台应充分利用云的算能算力优势，同时又满足对效率、时延、有效性等方面的要求，通过云边协同共同使能城轨行业数智化转型。

8.4.2 从数据存储角度，边缘计算平台宜存储的设备层大量和密度高的原始数据；信息管控平台宜存储经过边缘初步处理后用于进一步业务分析的数据。

8.4.3 从数据处理角度，边缘计算节点宜开展局部、实时、短周期的数据处理与分析，支撑边缘层业务的实时智能化决策与执行；信息管控平台宜开展全局性、非实时、长周期的大数据处理与分析，发挥长周期维护、业务决策支撑等领域优势。

8.4.4 从组织管理角度，融合模式下边缘计算平台应与信息管控平台应采用统一的技术架构，实现高效数据共享、业务协同、应用交付和集中运维。边缘计算平台应纳入信息管控平台的统一管理，包括应用部署、版本控制、风险监察、运营管理、数据治理等诸多方面。

9 安全要求

9.1 安全架构

城市轨道交通工业互联网管控系统网络安全实施框架主要从设备层安全、边缘计算层安全、企业层安全、行业层安全等方面开展建设。城市轨道交通运营单位主要完成设备层安全防护系统、边缘计算层安全防护系统、企业层安全防护系统等方面的建设。

工业互联网产业联盟 Alliance of Industrial Internet

城市轨道交通工业互联网管控系统网络安全设计框架

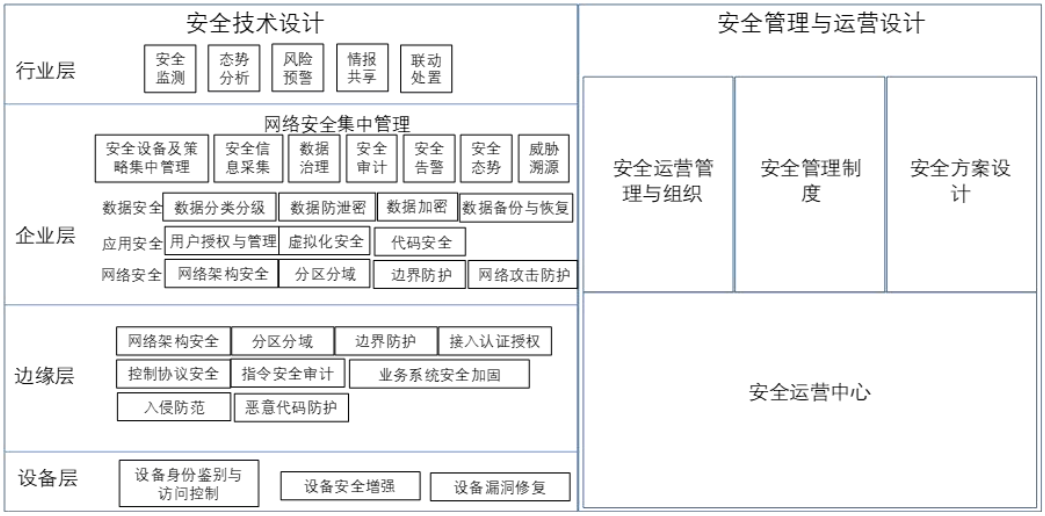

图 9　城市轨道交通工业互联网网络安全设计架构

9.2　安全措施

9.2.1　设备层防护

9.2.1.1　应建立车站控制设备安全措施，内容包括：

——控制设备自身应实现身份鉴别、访问控制和安全审计等安全要求，上位控制或管理设备实现同等功能或通过管理手段控制；

——应在经过充分测试评估后,在不影响系统安全稳定运行的情况下对控制设备进行补丁更新、固件更新等工作；

——应关闭或拆除控制设备的软盘驱动、光盘驱动、USB 接口、串行口或多余网口等,确需保留的应通过相关的技术措施实施严格的监控管理；

——应使用专用设备和专用软件对控制设备进行更新；

——应保证控制设备在上线前经过安全性检测,避免控制设备固件中存在恶意代码程序。

9.2.1.2　应建立车站设备身份鉴别措施，内容包括：

——应采用鉴别机制对接入工业互联网中的设备身份进行鉴别,确保数据来源于真实的设备；

——如存在需要对接入工业互联网中的设备进行远程管理的，应采取必要措施，防止身份鉴别信息在网络传输过程中被窃听；

——应对接入互联网的控制设备采取控制措施，包括实名接入认证、IP 地址与 MAC 地址绑定等。

9.2.1.3　应对车站设备建立访问控制措施，通过制定安全策略如访问控制列表，实现对接入工业互联网中设备的访问控制。

9.2.1.4　应建立运维用户身份鉴别措施，内容包括：

——应对登录设备进行运维的用户进行身份标识和鉴别，身份标识应具有唯一性，身份鉴别信息应具有复杂度要求并定期更换；

工业互联网产业联盟 Alliance of Industrial Internet

——对于登录设备进行运维的过程应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；
——应对登录设备进行运维的用户分配账户和权限；
——应重命名或删除默认账户，修改默认账户的默认口令；
——应及时删除或停用多余的、过期的账户，避免共享账户的存在；
——应对管理设备的用户授予其所需的最小权限,并实现对管理设备的用户的权限分离。

9.2.1.5 应建立设备层入侵防范措施，内容包括

——应遵循最小安装的原则，仅为设备安装需要的组件和应用程序；
——设备生产商应明示设备中使用的端口与服务列表及用途,并关闭设备中不需要的端口与服务；
——应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；
——应能发现可能存在的漏洞，并在经过充分测试评估后，及时修补漏洞。

9.2.2 边缘层防护

9.2.2.1 在车站边缘层应保障组网安全防护，建设内容包含：

——边缘层网络应采用冗余方案， 保障局域网网络通信的可用性；
——边缘层网络应与互联网、办公网络应采用隔离措施进行隔离；
——应根据承载业务的重要性对网络进行分区分域管理；
——应避免将信号系统、综合监控系统等重要网段部署在网络边界处；
——应采取必要的技术措施对不同安全域之间实施访问控制；
——应建立互联网接入审批和登记制度，严格控制互联网接入口数量,加强互联网接入口安全管理和安全防护。

工业互联网产业联盟
Alliance of Industrial Internet

9.2.2.2 在车站边缘层应建立边界保护，建设内容包括：

——应根据不同的业务系统划分不同的网络安全区域,按照管理和控制责任人的原则为各网络安全区域分配地址；
——应在网络边界根据访问控制策略设置访问控制规则,默认情况下除允许通信外受控接口拒绝所有通信；
——应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；
——不同的网络区域间应采用严格有效的、最小化的访问控制规则限制网络区域之间的网络通信，受控接口默认情况下除明确的业务需要允许通信外拒绝所有通信，禁止生产运营系统和互联网、企业办公网络等有 E-Mail、Web、Telnet、Rlogin、FTP 等通用协议通信。区域间访问控制设备应支持数据包访问控制检查规则，基于通信数据包的源地址、目的地址、源端口、目的端口和协议等进行访问控制；
——区域间访问控制设备应支持数据流访问控制检查规则,基于通信数据流的会话状态信息、应用协议和应用内容（包括常用工控协议 Modbus、OPC 协议等）等进行访问控制。

9.2.2.3 在边缘侧应采用安全的控制协议保障控制安全，可采取采用适当的加密措施、控制软件安全加固、指令安全审计等保障控制软件安全和控制协议安全，保证通信双方的信息不被第三方非法获取；

9.2.2.4 在车站边缘层业务系统应建立身份鉴别措施，建设内容包括：

——应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；
——应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；
——应采用安全方式防止用户鉴别认证信息泄露而造成身份冒用；
——当进行远程管理时，管理终端和车站边缘设备之间应建立双向身份验证机制。

9.2.2.5 在车站边缘层业务系统应建立访问控制措施，建设内容包括：

——应对登录的用户分配账户和权限，根据管理用户的角色分配权限，实现管理用户的权限分离，仅授予管理用户所需的最小权限；
——应重命名或删除默认账户，修改默认账户的默认口令；
——应及时删除或停用多余的、过期的账户，避免共享账户的存在；
——应对敏感信息资源设置安全标记，并控制主体对有安全标记信息资源的访问；
——应在不同等级的网络区域边界部署访问控制机制，设置访问控制规则。

9.2.2.6 在车站边缘层应建立入侵防范措施，建设内容包括：

——在车站边缘层应部署具备对控制系统与网络进行状态监测、日志采集与事件管理、流量采集与行为分析、异常告警及关联分析等功能的网络安全监测设备，及时发现、报告并处理包括设备状态异常、恶意软件传播、异常流量、异常诊断日志、端口扫描、暴力破解等网络攻击或异常行为。
——应在车站边缘层接入交换机处设置检测、防止或限制从外部发起的网络攻击行为；
——应在车站边缘层接入交换机处设置检测和限制从内部发起的网络攻击行为；
——应采取技术措施对网络行为进行分析，实现对网络攻击特别是未知的新型网络攻击的检测和分析；
——当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应提供报警；
——应能检测到针对城市轨道交通工业互联网系统的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等；
——应能检测到对虚拟网络节点的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等；
——应能检测到虚拟机与宿主机之间的异常流量，并进行告警。

工业互联网产业联盟 Alliance of Industrial Internet

9.2.2.7 在车站边缘层应建立恶意代码防范措施，建设内容包括：

——车站边缘层终端计算机应安装恶意代码防护软件，对恶意代码进行检测和清除，并及时更新恶意代码防护软件版本和恶意代码库；
——应采用免受恶意代码攻击的技术措施或可信验证机制对系统程序、应用程序和重要配置文件/参数进行可信执行验证，并在检测到其完整性受到破坏时采取恢复措施。

9.2.2.8 在车站边缘层应建立物联网设备接入安全管控措施，建设内容包括：

——应禁止通过互联网直接访问车站边缘层物联网设备；
——应在物理网络中通过 IP、MAC、端口绑定等技术限制非授权设备接入；
——应确保在远程管理时，采用由密码等技术支持的可信网络连接机制；
——应提供开放接口，允许接入可信的第三方安全产品；

——应确保在远程管理时，防止远程管理设备同时连接其他网络；
——应能够建立一条安全的信息传输路径，对网络中的安全设备或安全组件进行管理。

9.2.3 企业层防护

9.2.3.1 应建立企业层网络安全防护措施，内容包括：

——运营控制系统系统骨干网络、 局域网网络的网络带宽应满足业务高峰期及不同工作模式（如正常工况、阻塞工况、故障工况、 火灾工况和公共灾害工况控制模式）需要；
——骨干网网络和局域网网络相关设备（如骨干网的传输设备、 交换机、 路由器、 防火墙等，局域网的交换机、通信处理机和防火墙等）处理能力应满足业务高峰期和不同工作模式需要；
——骨干网网络应采用冗余方案（网络设备和通信线路的冗余），冗余设备宜分机柜放置，保障骨干网网络通信的可用性；
——网络安全管理应划分特定的网络区域， 与业务网络分离， 用于部署安全设备；
——应在企业侧网络内采取网络入侵检测措施， 有效检测已知网络攻击行为和未知新型网络攻击行为， 包括不限于端口扫描、强力攻击、 木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、 IP 碎片攻击、 网络蠕虫攻击和 APT 等攻击；
——当检测到攻击行为时， 应记录攻击源 IP、 攻击类型、 攻击目标、 攻击时间等信息， 并对严重入侵行为进行报警；
——应提供访问控制功能，对登录的用户分配账户和权限；
——应重命名或删除默认账户，修改默认账户的默认口令；
——应及时删除或停用多余的、过期的账户，避免共享账户的存在；
——应授予不同账户为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系；
——应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则；
——访问控制的粒度应达到主体为用户级，客体为文件、数据库表级、记录或字段级；
——应对敏感信息资源设置安全标记，并控制主体对有安全标记信息资源的访问；
——终端计算机应安装恶意代码防护软件，对恶意代码进行检测和清除，并及时更新恶意代码防护软件版本和恶意代码库；
——应采用免受恶意代码攻击的技术措施或可信验证机制对系统程序、应用程序和重要配置文件/参数进行可信执行验证，并在检测到其完整性受到破坏时采取恢复措施；
——应定期相关系统、 服务器、 工作站、 上位机、 网络设备、 安全设备、 控制设备等保障业务正常情况下进行漏洞扫描、 渗透测试或分析评估， 检测可能存在的已知漏洞，不应出现高风险漏洞；对漏洞进行充分测试评估并保留评估测试文档，及时修补或规避处理； 针对控制设备的补丁、 固件更新应不影响系统安全稳定运行； 控制设备的更新应使用专用设备和专用软件。

9.2.3.2 应建立企业侧应用安全防护措施，内容包括：

——应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，鉴别信息具有复杂度要求并定期更换；
——应提供并启用登录失败处理功能，多次登录失败后应采取必要的保护措施；
——应强制用户首次登录时修改初始口令；
——用户身份鉴别信息丢失或失效时，应采用技术措施确保鉴别信息重置过程的安全；

——应采用两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用动态口令、密码技术或生物技术来实现；
——应对企业侧采用的虚拟化等基础设施进安全加固，避免因为虚拟化安全问题引起应用系统不可用；对于采用虚拟化技术的业务，应保障不同业务之间的安全隔离，具备检测系统之间横向攻击的能力；
——应采用安全检查、安全评估等手段，保障业务系统代码安全缺陷识别，分析并找到这些问题引发的安全漏洞，保证业务系统上线前代码安全权限修订；
——应采用加密或数字签名等安全技术，保障资源访问的应用接口安全性；
——对外提供服务的 Web 接口应采用安全的数据传输协议来提高传输数据的安全性；
——对外提供服务的 API 接口应在调用前进行用户鉴别和鉴权，应确保接口访问控制的有效性；
——对外提供服务的 API 接口应具备防重放攻击、代码注入攻击、DOS/DDos 等攻击能力；
——当通信双方中的一方在一段时间内未作任何响应，另一方应能够自动结束会话；
——应能够对系统的最大并发会话连接数进行限制；
——应能够对单个账户的多重并发会话进行限制。

9.2.3.3 应在企业层应建立安全审计措施，内容包括：

——应在企业控制中心建立安全审计措施，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；
——审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；
——应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等；
——应确保审计记录的留存时间符合法律法规要求；
——应能对远程访问的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析。

工业互联网产业联盟
Alliance of Industrial Internet

9.2.3.4 应建立数据全生命周期安全防护措施，内容包括：

——应根据数据的种类、用途、敏感程度等建立数据分类分级原则；
——数据生成时，应根据数据的敏感程度进行分类分级，区分一般数据和敏感数据；
——应采用加密技术或其他保护措施实现鉴别信息的存储保密性；
——应支持用户实现对关键业务数据和管理数据的存储保密性；
——应支持用户对密码算法、强度和方式等参数的可选配置；
——应提供有效的磁盘保护方法或数据碎片化存储等措施，保证及时磁盘被窃取，非法用户也无法从磁盘中获取有效的用户数据；
——应能够检测到数据在存储过程中完整性受到破坏；
——应采用技术措施保证鉴别信息（指用于鉴定用户身份是否合法的信息，如用户登录各种业务系统的账号和密码、服务密码等）传输的保密性；
——应支持用户实现对关键业务数据和管理数据传输的保密性；
——应采用加密和认证技术确保从工业现场采集的数据的完整性和保密性；
——应能够检测到数据在传输过程中完整性受到破坏；
——应对数据的使用进行授权和验证；
——应使用校验码或密码技术确保虚拟机迁移过程中，重要数据的完整性，并在检测到完整性受到破坏时采取必要的恢复措施；

——应使用密码技术确保虚拟机迁移过程中，重要数据的保密性，防止在迁移过程中的重要数据泄露；
——应支持平台用户部署密钥管理解决方案，确保平台用户自行实现数据的加解密过程；
——应提供查询平台用户数据及备份存储位置的方式；
——平台用户应在本地保存其业务数据的备份；
——应保证不同平台用户的审计数据隔离存放；
——应为平台用户将业务系统及数据迁移到其他工业互联网平台和本地系统提供技术手段，并协助完成迁移过程；
——工业互联网平台的云存储服务应确保平台用户数据存在若干个可用的副本，各副本之间的内容应保持一致；
——应仅采集和保存业务需要的用户隐私信息；
——应禁止未授权访问和使用用户隐私信息。

9.2.3.5 应在企业侧建立集中安全管理措施，内容包括：

——针对企业侧的安全管理应划分特定的管理区域（如在控制中心），对企业侧相关的各站点、 车辆段、 停车场和控制中心的安全设备进行集中管控；
——应对相关的安全设备的安全策略（如防火墙访问控制策略、入侵检测系统策略等）、恶意代码规则库、 设备和系统补丁等安全相关事项进行集中管理；
——应能对系统网络中发生的各类安全事件进行识别、 分析和报警；
——应在企业部署安全信息采集探针，能够实时地对企业内部的安全动态信息进行有效采集，并进行有效汇总；
——应在网络出口的流量探针对企业内网进行扫描识别，发现并统计企业内网的资产并进行集中管理；
——应建立集中的安全审计服务器，集中管理企业侧历史操作事件及数据，发现能够改进系统性能和系统安全的方向，防止有意或无意的人为错误，防范和发现网络犯罪活动；
——企业侧应能及时发现资产中的安全威胁、实时掌握资产的安全态势；
——企业侧应具备安全处置跟踪能力，能够根据安全事件或安全资产溯源到相关责任人；
——企业侧应将收集到的相关数据进行分析统计，为企业做出相关研判提供依据。

9.2.4 行业层防护

9.2.4.1 在行业侧应建立轨道交通行业生产运营系统资产探测、流量分析、风险识别、态势分析、预警通报、应急处置能力。

9.2.4.2 在行业侧应建立轨道交通行业基础数据管理功能，能够与国家级平台建立连接通道，保障在安全事件发生时能够进行策略/指令下发、情报库共享、信息推送等功能。

9.3 安全运营与管理设计

9.3.1 应针对企业安全运营与管理组织进行建设，建设内容包括：

——应成立专门负责运营和管理城市轨道交通工业互联网管控系统信息安全工作的组织或职能部门，并成立信息安全工作领导小组，最高领导由单位主管领导委任或授权；
——应设立城市轨道交通工业互联网管控系统安全主管、安全运营、安全检查等各个方面的负责人岗位，并定义各负责人的职责；

——应设立城市轨道交通工业互联网管控系统管理员、网络管理员、安全管理员等岗位，并定义部门及各个工作岗位的职责。

9.3.2 应建立安全管理制度，建设内容包括：

——应对城市轨道交通工业互联网管控系统安全管理活动中的各类管理和运营内容建立安全管理制度；
——应对要求管理人员或操作人员执行的日常管理操作建立操作规程；
——应形成由安全策略、管理制度、操作规程、记录表单等构成的全面的城市轨道交通工业互联网管控系统信息安全管理和运营制度体系。

9.3.3 应针对城市轨道交通工业互联网管控系统安全方案进行设计，设计内容覆盖：

——工业互联网平台应提供开放接口或开放性安全服务，允许平台用户接入第三方安全产品或在平台选择第三方安全服务，支持异构方式对平台用户的网络、主机、应用、数据层的安全措施进行实施；
——应验证或评估城市轨道交通工业互联网管控系统所提供的安全措施的有效性。

9.3.4 应针对城市轨道交通工业互联网管控系统建立安全运营中心，建设内容覆盖：

——应建立安全运营中心，负责城市轨道交通工业互联网管控系统运行状态的监测和管理；
——安全运营中心需对城市轨道交通工业互联网管控系统中所有存储资源的访问权限作严格的控制，防止非法的用户未经授权的访问，避免数据泄密；
——应能够对城市轨道交通工业互联网管控系统内各类工业应用程序的通信协议进行有效识别和分析，防止基于工业协议的非法攻击行为的发生；
——应对安全运营中心中所有的系统在被访问时产生的日志，进行分析、统计和查询，管理员可以随 时监控用户的访问痕迹，来确保大数据平台访问的安全性；
——应对安全运营中心中各模块进行监控管理，实时掌握工业互联网平台的运行状况，保障大数据平台安全；
——应加强对安全运营中心的恶意代码和相关漏洞的筛查，保障其自身的安全；
——安全运营中心应遵循最小安装的原则，仅安装需要的组件和应用程序，并定期进行补丁更新及漏洞扫描，对发现的安全漏洞进行及时修补。

Alliance of Industrial Internet

参 考 文 献

[1] 中国城市轨道交通协会：《中国城市轨道交通智慧城轨发展纲要》
[2] AII联盟：《工业互联网体系架构（版本2.0）》

工业互联网产业联盟
Alliance of Industrial Internet