

中国城市轨道交通协会专家和学术委员会
城市轨道交通列车通信与运行控制国家工程实验室
呼和浩特地铁“用产学研”联合创新实验室
联合发布白皮书

白皮书编号：WP-2020001

城市轨道交通云平台建设实践经验白皮书

签发时间：2020年08月

签发版本：第一版（V1.0）

签发人：



中国城市轨道交通协会专家和学术委员会
城市轨道交通列车通信与运行控制国家工程实验室
呼和浩特地铁“用产学研”联合创新实验室

中国城市轨道交通协会是国家民政部批准设立的具有独立法人资格的全国性、行业性、非营利性社会组织，是我国城市轨道交通行业唯一的国家一级协会，也是国家 4A 级协会。协会由国家发展改革委主管，同时接受住房和城乡建设部、交通运输部、工业和信息化部等业务指导。协会现有会员单位 776 家，完整涵盖了城轨交通规划设计、建设施工、装备制造、运营管理等各个领域的企事业单位和科研教育机构。协会组建了由施仲衡院士领衔的专家和学术委员会。专家学术委共有委员 228 名，全部为行业内各专业领军人才。

城市轨道交通列车通信与运行控制国家工程实验室由交控科技股份有限公司牵头，采用“政产学研用”协同创新模式，联合北京交通大学、北京市轨道交通建设管理有限公司、北京地铁车辆装备有限公司共同申报，并经国家发改委批复成立的第一个国家级城轨信号系统科技平台。该平台将为国家建立一个国际领先的列控系统产业技术研发试验基地，提升城市轨道交通的自主创新能力和整体技术装备水平。

呼和浩特地铁“用产学研联合创新实验室”由呼和浩特市城市轨道交通建设管理有限责任公司牵头，联合华为技术有限公司、交控科技股份有限公司、北京交通大学共同成立，借助呼和浩特地铁现有的信息化基础环境以及对城轨云业务需求，在新技术应用和创新层面深度合作，持续保持在信息化创新方面的领先，为轨道交通建设管理运营持续注入业界先进技术和理念。

《城市轨道交通云平台建设实践经验白皮书》是中国城市轨道交通协会专家和学术委员会、城市轨道交通列车通信与运行控制国家工程实验室和呼和浩特地铁“用产学研”联合创新实验室的重大研究成果联合发布形式之一，旨在为城市轨道交通建设业主方提供决策依据，为设计方提供设计指南，为运营方提供运营维护指导。

对本书有任何问题或建议，欢迎与我们联系。

联系电话：010-52824660；邮箱：whitepaper@bj-tct.com

城市轨道交通云平台建设实践经验白皮书

法律声明

版权声明

本白皮书旨在向使用者与行业同仁提供技术信息。本白皮书及其衍生物（包括但不限于其他形式的文档格式、电子版本等）的版权归著作权人所有。

责任免除声明

本白皮书的有关城市轨道交通云平台建设实践技术的内容或图片等，版权归发布方所有。非平台建设实践范围内的产品或图片等，所有权及权益归其持有者所有。本白皮书出现的方法、示例代码等，均以“原样”提供，发布方不为其承担明示或者暗示的责任。

本白皮书是首次发布日期之版本，发布方保留在没有任何通知或者提示下对本白皮书的内容进行修改的权利。

您的建议有助于我们提高本白皮书的准确性、组织结构等，如若发现本白皮书存在任何错误，请与发布方取得直接联系。

前言

国家在 2019 年 9 月印发了《交通强国建设纲要》，纲要中指出，要“大力发展智慧交通。推动大数据、互联网、人工智能、区块链、超级计算等新技术与交通行业深度融合”，“构建泛在先进的交通信息基础设施。构建综合交通大数据中心体系，深化交通公共服务和电子政务发展”。这为我们国家交通行业的未来发展指明了方向。

截止到 2019 年年底，国内共有 40 个城市开通了城市轨道交通运营线路 208 条，运营线路总长度 6736.2 公里。我国已经是一个无可争议的轨道交通大国。中国城市轨道交通协会经过近两年的研究于 2020 年 3 月发布了《中国城市轨道交通智慧城轨发展纲要》（以下简称《纲要》）。《纲要》既是对交通强国战略的响应，同时也提出了适合中国城轨行业发展的具体方针和战略。《纲要》提出了 1-1-8-1 的智慧城轨发展蓝图，即在城轨云和大数据平台上，重点发展 8 个智能化智慧化体系。

《纲要》指出“信息化建设是智慧城轨建设的基础”，在《纲要》编制阶段，同步进行城轨信息化规范体系的顶层设计，建立并逐步发布“1352”四个层级组成的《中国城轨信息化规范体系》”。2019 年 9 月发布的《智慧城市轨道交通信息技术架构及网络安全规范》是针对城轨云提出的顶层规范性文件，而呼和浩特城轨云平台就是这一规范的首次成功实践。

为了能更好的推动智慧城轨的落地，中国城市轨道交通协会专家和学术委员会、城市轨道交通列车通信与运行控制国家工程实验室和呼和浩特地铁“用产学研”联合创新实验室总结建设经验，提取关键技术，形成《城市轨道交通云平台建设实践经验白皮书》，作为未来城轨云建设工作的参考。

主要编写人：刘占英、朝鲁、张振义、陈瑞军、刘超、李申、孟伟君、楚研、樊艳、刘楠、杨瑞超、刘海建、张瑞雪、王彪、牛昌平、谢泽宇、李致兴、沈光亮

主要审查人：李中浩、邢智明、张建明、王伟、娄永梅、何晶、张义鑫、侯久望、巴图、郭新灵

目录

法律声明.....	2
前 言.....	3
1. 引言.....	8
1.1. 术语和定义.....	8
1.2. 缩略语.....	10
1.3. 引用文件及设计规范.....	11
2. 概述.....	14
2.1. 标准城轨云架构.....	14
2.2. 国内城轨云建设情况.....	16
3. 城轨云平台.....	17
3.1. 平台设计.....	17
3.1.1. 整体架构.....	17
3.1.2. 云平台区域划分与设置.....	21
3.1.3. 城轨云平台管理.....	24
3.1.4. 功能及服务.....	27
3.1.5. 业务降级及线路扩展.....	30
3.2. 网络设计.....	31
3.2.1. 网络整体架构.....	32
3.2.2. 安全生产网.....	33
3.2.3. 内部管理网.....	35
3.2.4. 外部服务网.....	36
3.2.5. 三网横向流量.....	37
3.2.6. 站场段网络.....	38
3.2.7. 双中心网络.....	39
3.2.8. 运维管理网.....	40
3.2.9. 其它网络.....	40
3.3. 资源设计.....	41
3.3.1. 计算资源.....	41
3.3.2. 存储资源.....	43
3.4. 桌面云设计.....	45
3.4.1. 硬件部署架构.....	45
3.4.2. 桌面云计算资源规划.....	46
3.4.3. 桌面云存储资源规划.....	47
3.4.4. 桌面云网络规划.....	48
3.5. 灾备及备份.....	48
3.5.1. 容灾简介.....	48
3.5.2. 容灾关键技术.....	50
3.5.3. 城轨云业务容灾.....	52
3.6. 网络安全.....	55
3.6.1. 等保 2.0 标准.....	56
3.6.2. 安全管理设备.....	63
3.6.3. 城轨云安全边界.....	64

3.6.4.	信息安全部署框架.....	67
3.6.5.	呼和浩特城轨云等保评测.....	73
3.7.	云平台应用部署实例.....	85
3.7.1.	ATS、ISCS 部署网络结构优化.....	85
3.7.2.	云上组播结构优化.....	86
3.7.3.	ATS 系统在云上可用性指标的计算.....	87
3.7.4.	ATS 上云的 SIL 等级合规方案.....	91
3.7.5.	业务系统互联关系.....	92
3.7.6.	典型业务系统部署实例.....	94
4.	大数据平台.....	108
4.1.	大数据平台总体架构.....	108
4.2.	数据集成层.....	110
4.3.	数据存储+应用支撑层.....	112
4.4.	数据应用.....	113
4.4.1.	运营管理类应用.....	113
4.4.2.	设备监测及运维类应用.....	122
5.	基础设施配套设计.....	128
5.1.	机房设备布置的设计原则.....	128
5.2.	机房设计.....	129
5.2.1.	主用中心布置方案及呼和浩特云平台实例.....	129
5.2.2.	网络设备布置原则.....	130
5.2.3.	计算设备布置原则.....	132
5.3.	模块化机房.....	134
5.3.1.	模块化机房简介.....	135
5.3.2.	冷通道/热通道.....	135
5.3.3.	制冷方式.....	136
5.3.4.	UPS 供电.....	137
5.3.5.	消防联动.....	138
5.4.	PUE 计算.....	138
5.4.1.	PUE 指标测量点.....	138
5.4.2.	能耗的间接测量和估算.....	139
6.	城轨云测试平台.....	141
6.1.	设计原则.....	141
6.2.	测试平台设计.....	143
6.3.	测试范围.....	145
6.3.1.	云平台自测试.....	145
6.3.2.	业务系统功能及兼容性测试.....	145
6.3.3.	系统性能测试.....	146
6.3.4.	灾备测试.....	146
6.4.	测试总结.....	147
7.	工程实施.....	148
7.1.	设备安装.....	148
7.1.1.	施工前检查.....	148
7.1.2.	安装工艺.....	148

7.1.3.	施工组织.....	150
7.2.	系统调试.....	151
7.2.1.	测试平台.....	151
7.2.2.	云平台搭建.....	152
7.2.3.	业务系统资源发放.....	153
7.3.	联合调试.....	153
7.3.1.	业务系统与云平台联调.....	153
7.3.2.	安全调试.....	154
7.3.3.	容灾及故障测试.....	154
7.3.4.	业务系统数据备份.....	155
7.4.	项目验收.....	155
7.4.1.	验收内容.....	155
7.4.2.	验收检查标准.....	157
7.5.	典型问题.....	162
7.5.1.	设计阶段.....	162
7.5.2.	测试平台测试阶段.....	163
7.5.3.	设备安装阶段.....	163
7.5.4.	系统调试阶段.....	163
7.5.5.	联合调试阶段.....	164
8.	城轨云运维.....	165
8.1.	日常运维.....	165
8.2.	安全防护.....	166
8.3.	运维架构.....	166
8.4.	应急演练.....	169
9.	呼和浩特城轨云建设实践.....	171
9.1.	顶层设计.....	171
9.2.	方案论证.....	172
9.3.	科研立项.....	174
9.4.	工程落地.....	174
9.4.1.	实施历程.....	174
9.4.2.	供货管理.....	176
9.4.3.	安装管理.....	177
9.4.4.	调试管理.....	178
9.4.5.	验收管理.....	181
9.4.6.	企业管理.....	182
9.4.7.	资源管理.....	182
9.5.	未来方向.....	183
10.	附录.....	185
10.1.	测试结果.....	185
10.1.1.	云平台自测试结果.....	185
10.1.2.	业务系统功能及兼容性测试结果.....	185
10.1.3.	系统性能测试结果.....	185
10.1.4.	灾备测试结果.....	200
10.2.	IP 地址规划.....	204

10.2.1.	线路级地址划分.....	204
10.2.2.	线网级地址划分.....	215
10.3.	接口技术要求.....	217
10.3.1.	接口界面.....	217
10.3.2.	测试分工.....	229
10.4.	参与单位及主要技术人员名单.....	231

1. 引言

1.1. 术语和定义

下列术语和定义适用于本文件。

信息系统 Information System

运用于轨道交通领域的由计算机软件、硬件及其他外围设备组成的以处理信息为目的的人机一体化系统，包括了控制系统、监测系统、信息管理系统、决策支持系统。

主用中心 Operation Center

可称为业务中心或者信息中心，主用系统所在的数据中心，可对外提供相应的数据或者信息服务。

灾备中心 Backup Center for Disaster Recovery

即灾难备份中心，用于灾难发生后接替主用系统进行数据处理和支持关键业务功能运作的备用数据中心。

线网骨干网 Backbone Network

是连接轨道交通主用、灾备中心及各线路中心等主要业务节点之间的主干传输系统。

基础设施即服务 Infrastructure as a Service

云平台提供的一种服务。云平台为用户部署操作系统、应用程序提供的一种物理或虚拟化的计算、存储、网络等IT基础设施资源环境和平台服务。

平台即服务 Platform as a Service

云平台提供的一种服务。云平台提供稳定在线的开发/测试环境、中间件、数据库等平台软件服务，用户通过网络接口即可实现软件开发/测试功能，为上层应用提供中间件调用、数据库访问等功能。

软件即服务 Software as a Service

云平台提供的一种服务。云平台提供稳定在线的应用软件服务，用户通过网络接口、使用客户端软件即可实现应用软件访问功能。

数据中心 Data Center

为集中放置的电子信息技术设备提供运行环境的建筑场所，可以是一栋或几栋建筑物，也可以是一栋建筑物的一部分，包括主机房、辅助区、支持区和行政管理区等。

瘦终端 Thin Terminal

指在云桌面部署模式下，可通过各种协议连接到运行在服务器上的桌面设备。

安全生产网 Safety Production Network

用于承载为城市轨道交通一线生产及调度人员服务的运营生产类业务应用系统的计算机网络。

内部管理网 Internal Management Network

用于承载城市轨道交通运营管理、企业管理、建设管理、资源管理等面向企业内部用户服务的业务应用系统的计算机网络。

外部服务网 External Service Network

用于承载城市轨道交通乘客服务类等面向外部或公众服务的计算机网络。

信息安全等级保护 Multi-Level Protection of Information Security Scheme

指对信息和信息载体（信息系统所涉及的操作系统、数据库、应用系统、网络系统等）按照重要性等级分级别进行保护。

虚拟数据中心 VDC, Virtual Data Center

是IaaS资源的逻辑抽象，用于对可用的CPU、内存资源、存储和网络进行管理。VDC保证了按需使用资源、资源隔离以及自助管理。一个企业下属很多组织，每个组织可以设定一个或多个VDC，每个VDC上面可以针对企业业务，部署不同的应用。可以根据企业需求和业务需求，对不同的VDC配备不同服务质量的资源，并对这些不同资源配置进行管理。

虚拟专有云 VPC, Virtual Private Cloud

是一套逻辑隔离的、由用户自主配置和管理的虚拟网络环境，旨在提升用户资源的安全性，简化用户的网络部署。用户可以在VPC中自由选择IP地址范围、创建多个子网、自定义安全组以及配置路由表和网关等，方便地管理和配置网络，进行安全、快捷的网络变更。同时，通过自定义安全组内与组间实例的访问规则以及防火墙等多种安全层，加强对子网中实例的访问控制。

区域 Region

一般指地理上完全独立的区域，Region之间资源完全隔离，以实现最大程度的容错能力和稳定性。同一个Region内共享对象存储、VPC网络、弹性IP、镜像等公共服务。由于Region内设备之间管理流量、存储流量、业务流量较大，对网络带宽有较高的要求，不推荐Region跨物理数据中心。

可用分区 AZ, Available Zone

是在区域之下，一个包含特定物理资源（计算、存储、网络）的逻辑结构。可用分区内的物理资源共享了可靠性故障点，比如共享相同的机电基础设施（如空调，UPS），通信资源（如交换机）。用户如果要提高AZ的可靠性，就要把更高可靠性的冗余资源部署到不同的可用分区。

大数据平台 Big Data Platform

实现网域内部的数据交换和共享，以及安全生产网与内部管理网、外部服务网跨网域之间的数据交换和共享；并在共享数据的基础上提供大数据分析功能，实现对各类业务应用系统大数据分析应用技术支持的平台。

固态硬盘 SSD, Solid State Drive

固态硬盘用固态电子存储芯片阵列而制成的硬盘，由控制单元和存储单元组成，固态硬盘在接口的规范和定义、功能及使用方法上与普通硬盘的完全相同。固态硬盘具有速度快，不易损坏等优点。

机械硬盘 HDD, Hard Disk Drive

机械硬盘又称为温彻斯特硬盘，主要由盘片、磁头、盘片转轴及控制电机、磁头控制器、数据转换器、接口、缓存等几个部分组成。机械硬盘具有容量大，价格相对低廉等优点。

列车自动控制 Automatic Train Control

信号系统自动实现列车监控、安全防护和运行控制技术的总称。

列车自动监控 Automatic Train Supervision

根据列车时刻表为列车运行自动设定进路，指挥行车，实施列车运行管理等技术的总称。

列车自动防护 Automatic Train Protection

自动实现列车运行安全间隔、超速防护、进路安全和车门等监控技术的总称。

列车自动运行 Automatic Train Operation

自动实行列车加速、调速、停车和车门开闭、提示等控制技术的总称。

全自动运行系统 Fully Automatic Operation system

运行在有人值守的全自动运行或无人值守的全自动运行下的城市轨道交通系统。

1.2. 缩略语

下列缩略语适用于本文件

ATC：列车自动控制（Automatic Train Control）

ACS：门禁系统(Access Control System)

AFC: 自动售检票系统(Automatic Fare Collection)

CBTC: 基于通信的列车控制 (Communication Based Train Control)

DDoS: 分布式拒绝服务(Distributed Denial of Service)

FC : 光纤通道 (Fibre Channel)

FTP : 文件传输协议 (File Transfer Protocol)

ISCS: 综合监控系统 (Integrated Supervisory Control System)

IP: 网络互连协议 (Internet Protocol)

IPS: 入侵防御系统(Intrusion Prevention System)

LTE: 长期演进技术 (Long Term Evolution)

OA: 办公自动化(Office Automation)

OCC: 线路控制中心 (operating control center)

OLP: 光纤线路自动切换保护装置 (Optical Fiber Line Auto Switch Protection Equipment)

OMSP: 光复用段保护 (Optical Multiplex Section Protect)

OTN: 光传送网 (OpticalTransport Network)

PIS: 乘客信息系统 (Passenger Information System)

SAN: 存储局域网络(Storage Area Network)

SDN: 软件定义网络 (Software Defined Network)

SLA: 服务等级协议(Service-Level Agreement)

VPN: 虚拟专用网络 (Virtual Private Network)

1.3. 引用文件及设计规范

所有设备、材料、施工工艺及施工符合下面所列规范和设计要求:

GB / T 21562.2—2015 轨道交通可靠性、可用性、可维修性和安全性规范及示例

GB / T 28808—2012 轨道交通通信、信号和处理系统控制和防护系统软件

GB / T 28809—2012 轨道交通通信、信号和处理系统信号用安全相关电子系统

GB / T 22239—2019 信息安全技术 网络安全等级保护基本要求

GB / T 28448—2019 信息安全技术 网络安全等级保护测评要求

GB / T 25070—2019 信息安全技术 网络安全等级保护安全设计技术要求

GB / T 32399—2015 信息技术 云计算 参考架构

GB / T 32400—2015 信息技术 云计算 概览与词汇

GB / T 34942—2017 信息安全技术 云计算服务安全能力评估方法

GB / T 34982—2017 云计算数据中心基本要求

GB / T 36325—2018 信息技术 云计算 云服务级别协议基本要求

GB / T 36326—2018 信息技术 云计算 云服务运营通用要求

GB / T 37738—2019 信息技术 云计算 云服务质量评价指标

GB / T 37938—2019 云资源监控指标体系

GB 50157—2013 地铁设计规范

GB 50174—2017 数据中心设计规范

GB 50300—2013 建筑工程施工质量验收统一标准

GB 50303—2015 建筑电气工程施工质量验收规范

GB 50311—2016 综合布线系统工程设计规范

GB 50490—2009 城市轨道交通技术规范

GB 50174—2017 数据中心机房设计规范

GB 2887—2011 计算机机房场地通用规范

GB 50462—2015 数据中心基础设施施工及验收规范

GB 50054—2011 低压配电设计规范

GB 50052—2009 供配电系统设计规范

GB 50034—2013 建筑照明设计标准

GB 50736—2012 民用建筑供暖通风与空气调节设计规范

GB 50016—2014 建筑设计防火规范

GB 50222—2017 建筑内部装修设计防火规范

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第1部分总体需求

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第2部分技术架构

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第3部分网络安全

《城市轨道交通云平台构建技术规范》（送审稿）

《城市轨道交通大数据平台技术规范》（送审稿）

《城市轨道交通云平台网络拓扑架构技术规范》（送审稿）

《城市轨道交通云平台网络安全技术规范》（送审稿）

《城市轨道交通线网运营指挥中心系统技术规范》（送审稿）

其它有关的现行国家、国际、行业标准。

2. 概述

云计算从 2006 年美国亚马逊 AWS 开始，到今天经过了十几年时间，经历了萌芽、探索、发展时期，已经进入繁荣和成熟期。2019 年全球公有云市场规模超越 2 千亿美元。“上云”已成为企业加快数字化转型、鼓励技术创新和促进业务增长的第一选择。

在这样的技术潮流下，中国城市轨道交通协会（以下简称“协会”）组织编纂了《智慧城市轨道交通信息技术架构及网络安全规范》（以下简称“《规范》”），作为指导行业内建设实施城轨云的顶层规范。呼和浩特城市轨道交通云平台（以下简称“呼和浩特城轨云”）的工程实践，不仅依照协会规范进行设计和实施，更是对现有标准的验证，并为将来的智慧业务提供可靠的底层基础平台。

《城市轨道交通云平台建设实践经验白皮书》（以下简称“白皮书”）对现有规范进行了全方面的验证，包括：对信号系统上云可用性、可靠性的验证；对全路网统一 IP 规划的验证；对城轨云与其它非云系统互联互通的验证；对三网统一云管的验证；对三大网域（安全生产、内部管理、外部服务）安全隔离的验证；对承载灾备中心功能的验证；对站段云功能的验证；对全网信息安全保护的验证等，并提供了典型机房设计的基线参考。

本白皮书的编制原则是源于规范实于规范，在对呼和浩特城轨云既有经验总结的基础上，对部分功能提出了优化建议。本白皮书目标是为建设一个安全、稳定、高效的城市轨道交通云平台（以下简称“城轨云”）提供参考。

2.1. 标准城轨云架构

《规范》共分成3个分册：《总体需求》、《技术架构》及《网络安全》。

- 1) 总体需求部分规定了智慧城市轨道交通信息技术系统的总体需求，包括总体架构，应用系统功能，对云平台、系统软件、系统备份、系统容灾、系统网络、系统安全及RAMS保障等的需求。
- 2) 技术架构部分规定了智慧城市轨道交通信息技术系统的云计算平台架构、大数据平台架构、网络架构、数据中心及环境要求、运维体系。
- 3) 网络安全部分规定了智慧城市轨道交通信息技术系统的网络安全架构、边界安全要求、云计算环境安全要求、主要业务系统安全要求。

城市轨道交通信息技术系统总体架构见下图：



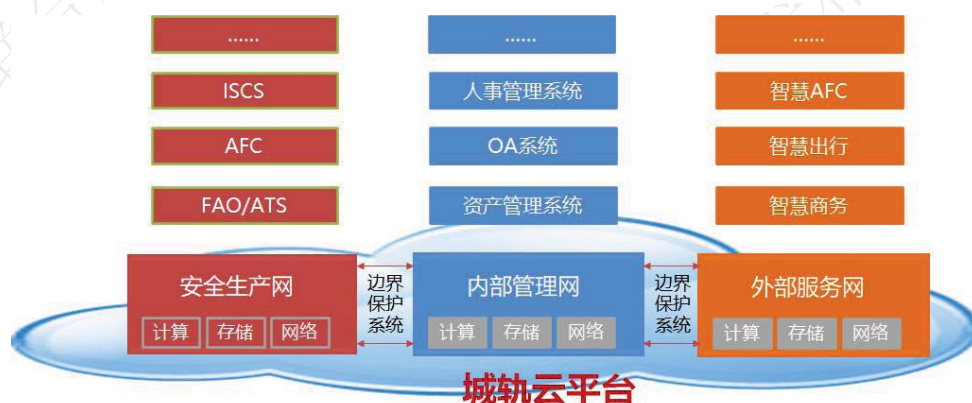
(来源:《规范》第1部分:总体需求)

通过搭建城市轨道交通统一云平台,纳管主用中心、同城异地灾备中心、站段云,依托安全生产网、内部管理网、外部服务网,拓展运营生产、运营管理、企业管理、建设管理、资源管理等领域,构建运营生产(应急指挥)中心、企业管理中心和乘客服务管理中心,打造轨道交通企业的门户网站。

《规范》要求智慧城市轨道交通云平台总体上符合下列规定:

- 1) 云平台系统至少应为安全生产网、内部管理网、外部服务网各应用系统提供IaaS服务,可分系统、分阶段为各应用系统提供PaaS、SaaS服务;
- 2) 安全生产网内各应用系统的服务器可通过云平台虚拟化部署在云计算资源池中;重要应用系统可在车站级部署物理服务器,作为车站降级处理使用;
- 3) 云平台可统一考虑为中心级、车站级调度人员及集团办公人员等配置瘦终端及云桌面,3D建模、大视频流等终端应用可不采用云桌面。

城轨云平台为安全生产网,内部管理网、外部服务网各应用主要以IaaS服务为核心,逐步分系统、分阶段提供PaaS、SaaS服务。



城轨云平台可为安全生产网内的如下系统提供资源，包括：大数据平台系统、信号ATS系统、自动售检票系统、综合监控系统、门禁系统、乘客信息系统、专用电话系统、LTE-M系统、车辆智能运维系统和线网运营指挥中心系统等。

可为内部管理网的如下系统提供资源，包括：大数据平台系统、运营管理系统、企业资源管理系统、资源管理系统、建设管理系统、企业内部网站、协同办公系统、邮件系统、ERP系统、BIM管理系统、物资管理系统、站务管理系统和乘务管理系统等。

可为外部服务网的如下系统提供资源，包括：大数据平台系统、乘客服务管理系统、线网智慧客流组织系统、视频监控系统、企业门户系统、公务电话系统和互联网售检票系统等。

2.2. 国内城轨云建设情况

国内多地在协会的《规范》指引下，已经开始建设或计划建设城轨云平台。如深圳地铁6、10号线采用单线路综合云技术方案，综合云平台融合ISCS、CCTV、ACS、PIS等多个系统，计划2020年开通。深圳14、16号线已规划多线路多专业云平台方案，包括信号FAO在内的多个应用系统均部署在此平台。武汉地铁规划将32条线路纳入城轨云平台。此外，西安、济南、南宁等多个城市都有建设城轨云平台的计划。

呼和浩特城轨云是国内第一个成功开通的多线路、多专业的综合城轨云平台。呼和浩特城轨云工程分为前期预研、工程设计和工程实施3个阶段，执行周期4年，已于2019年12月30日正式投入使用。

3. 城轨云平台

3.1. 平台设计

3.1.1. 整体架构

云计算在城轨行业的引入，将更加有效实现信息系统的技术标准化和管理规范化，为企业信息系统提供更好的支持。云计算架构中，通过虚拟化技术将物理上分散的服务器、网络设备、存储设备，逻辑上形成资源池，而将这些资源以灵活、动态、可管理的方式提供给用户，离不开云计算的“大脑”——云管理平台。

为确保业务高可靠，在数据中心级云计算平台上规划生产、灾备双中心；通过 OTN 设备打通主备双中心间网络，利用云管理平台的统一管理，实现“物理分散，逻辑集中”的分布式云数据中心建设。

一、主用中心

主用中心作为城市轨道交通线网级云平台的主服务中心，在线路正常的时候承担主服务功能。按照主用中心承载的业务类型、安全等级、网络隔离要求等因素，将平台分为安全生产网、内部管理网、外部服务网以及用于平台维护的运维管理网，四个网域之间利用边界防火墙或者网闸进行隔离。

1. 安全生产网

主要承载运营生产相关业务系统，其提供虚拟化资源池、物理机资源池、桌面云、备份系统等，以及完整的非云接入、终端接入、线路汇聚。安全生产网作为核心区域，贯穿中心及站段，应优先建设。安全生产网具备资源发放条件时，逐步配合业务系统进行业务部署，以及云内、非云网络对接。

安全生产网部署的业务系统包括：

- 列车自动监控系统
- 综合监控系统
- 自动售检票系统
- 门禁系统
- 乘客信息系统
- 通信集中告警系统
- 数据挖掘系统

- 其他系统

2. 内部管理网

主要承载企业管理相关业务系统，其提供虚拟化资源池、桌面云。内部管理网作为承载企业管理业务的区域，其不与行车控制直接相关。

内部管理网部署的业务系统包括：

- 资产管理系统
- 企业内部网站
- 协同办公系统
- 邮件系统
- ERP 系统
- 合同管理系统
- BIM 管理系统
- 物资管理系统
- 设备维护工作管理系统
- 施工调度管理系统
- 运营日报系统
- 站务管理系统
- 乘务管理系统
- 其他系统

3. 外部服务网

主要承载乘客服务相关业务系统，当业务规模不大时，可采用虚拟化解决方案。外部服务网承载互联网售检票业务与日常运营相关业务。

外部服务网部署的业务系统包括：

- 邮件系统
- 外部网站
- 互联网购票子系统手机 APP 平台
- 公务电话

4. 运维管理网

主要承载网管、运维、安全相关的管理系统。

运维管理网部署的业务系统包括：

- 网管系统，主要是网管设备
- 网络安全，主要是全网域的安全管理设备（如终端准入，日志审计，运维审计堡垒机等）。根据实际项目的设计和需求，安全管理中心，态势感知等安全管理设备也可以部署在运维管理网。
- 运维管理，云平台运维、大数据平台运维，作为全网域应用，均建议部署在运维管理网。

二、灾备中心

灾备中心作为城市轨道交通线网级云平台的备用中心，在主用中心故障的时候承担备用功能。与主用中心划分方式一致，灾备中心同样划分为安全生产网、内部管理网、外部服务网以及用于平台维护的运维管理网，四个网域之间利用边界防火墙或者网闸进行隔离。灾备中心主要用于主用中心故障时的备用功能，因此，灾备中心仅承载有容灾要求的部分业务系统。

灾备中心云平台主要为灾备模式下安全生产网的列车自动监控系统提供所需的计算、存储、网络资源，为综合监控系统、自动售检票系统、乘客信息系统、门禁系统以及内部管理网、外部服务网的系统业务提供所需的存储资源。

三、站段云

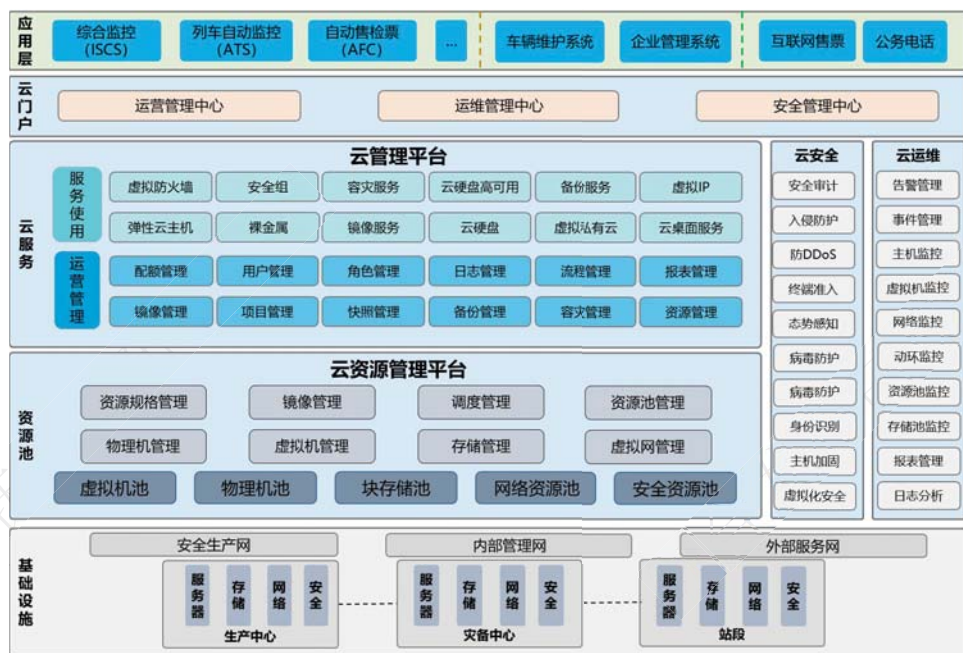
站段云为部分安全生产网业务在站段提供运行环境，实现车站业务与中心云平台计算、存储的数据交互。当车站与主用中心云平台、灾备中心云平台失去联系时，站段云可为安全生产网业务（包括：综合监控系统、自动售检票系统、乘客信息系统）提供降级模式下所需的计算、存储、网络、安全等资源，为业务系统降级应急处理提供基础条件功能，站段云平台纳入中心云平台的统一管理，通过云平台保证资源的快速交付和统一管理，支撑业务快速上线、融合运营、统一运维。

四、网络安全

城轨云的网络安全防护包括一个中心（安全管理中心）、三重防护（区域边界安全防护、通信网络防护、计算环境防护）。城轨云共计 14 个安全逻辑边界需要保护，均包含在整体安全防护框架内，后续有专门章节论述城轨云网络安全。

城轨云平台是以构建基础设施资源池（IaaS）为核心，搭建企业级应用、开发、数据平台（PaaS），预留未来以软件为交付单元（SaaS）的扩展能力。城轨云中，主要分为云资源管理平台和云管理平台。云资源管理平台通过 API 接口对主用中心、灾备中心和站段云中计算资源、存储资源、网络资源等在内的基础设施进行管理，逻辑上抽象为可灵活切割、分配的资源池，并根据上层用户动作将其转换为配置指令并通过相关组件实现动态配置。云管理平

台是在云资源管理平台之上，将基础设施封装为相关服务，以服务目录的方式展示给用户。用户通过申请、提交、审核等操作，实现购物般的方便体验，只需通过简单的页面点击即可完成资源发放、变更、回收等全生命周期管理。



城轨云平台环境下，业务系统对于云服务的诉求仍以基础设施服务为核心。因此，城轨云平台的建设是以 IaaS 平台为主，逐步扩展 PaaS、SaaS。

城轨云平台按功能分区可划分为：基础设施层、资源池层、云服务层、云安全、云运维、云门户层等。

- 1) 基础设施层：作为云平台的底座，云平台将分散在主用中心、灾备中心、站段的资源统一纳管，划分安全生产网、内部管理网、外部服务网。在三张网基础上“化零为整”构建云资源池。
- 2) 资源池层：资源池层可以接入计算（虚拟机池、物理机池）、存储（块存储资源池）、网络资源池以及安全资源池。
- 3) 云服务层：通过对资源池层的封装，实现云资源服务的发现、编排、发放等功能，体现了从资源到服务的转换，是云管理平台对外呈现服务的主要方式；用户通过运营管理中心或管理员通过运维管理中心，可实现对服务的分配、使用、监控等生命周期管理。
- 4) 云安全层：通过提供全方位、多粒度的安全防护措施，为平台及业务提供安全服务。
- 5) 云运维层：提供对多数据中心的统一运维管理，包括资源运维管理、告警管理、拓扑管理、性能管理等。
- 6) 云门户层：城轨云平台通过将多种资源进行物理、逻辑整合，通过运营中心、运维中心、安全中心提供服务能力。

3.1.2. 云平台区域划分与设置

3.1.2.1. Region、AZ、VDC、VPC 之间的关系

基于 OpenStack 架构的城轨云平台，会有 4 个平台配置的基本概念：区域（Region），可用分区（Available Zone，简称 AZ），虚拟数据中心（Virtual Data Center，简称 VDC）和虚拟私有云（Virtual Private Cloud，简称 VPC）。

这 4 个概念分属不同层面，其中 Region 和 AZ 的概念首先由亚马逊云服务（AWS）提出，OpenStack 项目继承了这个架构。它们均偏地理概念，是对云平台物理资源的一种划分方式。在其它 IT 架构下（如 VMware 或其它厂商的虚拟化架构）划分物理资源的方式并不完全相同，须根据项目的实际情况进行配置。

VDC 和 VPC 更多的是针对虚拟资源划分和网络隔离。在城轨云的环境下，他们之间的关系如下：

$$\text{VDC} : \text{AZ} = m : n$$

$$\text{VPC} : \text{AZ} = m : n$$

$$\text{Region} : \text{AZ} = 1 : m$$

一个 Region 可以包含多个 AZ。AZ 包含于 Region，AZ 不可跨越 Region。VDC 或 VPC 都可跨 AZ 设置。

以呼和浩特城轨云具体配置举例：

在主用中心安全生产网的 region 下，依照主机类型分成云主机 AZ、裸金属 AZ，即 AZ 是按照物理资源的属性进行划分。但在设置某个业务系统 VDC 资源的时候，会同时包含云主机 AZ 和裸金属 AZ 中的资源，VPC 设置也会包含云主机 AZ 和裸金属 AZ 的网络。这些设置应用系统无感知，属于云平台自身配置。后续章节有呼和浩特城轨云配置信息更详尽的描述。

承载具体应用的 VDC（如某个线路级应用）中一定会包含一个 VPC，管理级别的 VDC（如安全生产网这种 VDC）不包含 VPC。

3.1.2.2. Region 及 AZ 划分

主用中心、灾备中心的网域划分与承载的业务系统类型、重要程度、保护等级等因素有关，因此，对与双中心区域（Region）划分可与网域划分一致，即：外部服务网、内部管理网、安全生产网。Region 与网域划分一致，便于管理，可对不同类型业务系统提供不同的可靠性保护。同时在建设时可按照网域优先级进行建设。Region 命名可根据网域的首字母拼音来命名，如主用中心安全生产网为 AQSC1，灾备中心安全生产网为 AQSC2，主用中心内部管理网为 NBGL1，灾备中心内部管理网为 NBGL2，主用中心外部服务网为 WBFW1，灾备

中心外部服务网为 WBFW2。

Region 的设置还与实际部署有关：1、相关网域是否真实资源部署，2、相关网域是否配置了 OpenStack 的云平台系统。如果此网域没有设备，或是使用虚拟化平台（非 OpenStack）可不用考虑 Region 和 AZ 的设置。

每个 Region 下，按需可分成 3 个 AZ：云主机（KVM，Kernel-based Virtual Machine）、裸金属（BMS，Bare Metal Server）、数据挖掘（DM，Data Mining）。可以使用 Region+AZ 的组合来命名。以主用中心的安全生产网为例，则 AZ 名称分别是：云主机 AZ：AQSC1_KVM_AZ，裸金属 AZ：AQSC1_BMS_AZ，数据挖掘 AZ：AQSC1_DM_AZ。

数据中心	网域	区域/region	AZ	备注
主用中心	安全生产网	安全生产网 AQSC1	云主机 AZ AQSC1_KVM_AZ	按需调整
			裸金属 AZ AQSC1_BMS_AZ	
			数据挖掘 AZ AQSC1_DM_AZ	
	内部管理网	内部管理网 NBGL1	云主机 AZ NBGL1_KVM_AZ	
			裸金属 AZ NBGL1_BMS_AZ	
			数据挖掘 AZ NBGL1_DM_AZ	
	外部服务网	外部服务网 WBFW1	云主机 AZ NBGL1_KVM_AZ	
			裸金属 AZ NBGL1_BMS_AZ	
			数据挖掘 AZ NBGL1_DM_AZ	
灾备中心	安全生产网	安全生产网	云主机 AZ	

		AQSC2	AQSC2_KVM_AZ	
			裸金属 AZ	
			AQSC2_BMS_AZ	
	内部管理网	内部管理网	云主机 AZ	
		NBGL2	NBGL2_KVM_AZ	
	外部服务网	外部服务网	云主机 AZ	
		WBFW2	WBFW2_KVM_AZ	

3.1.2.3.VDC 及 VPC 设置

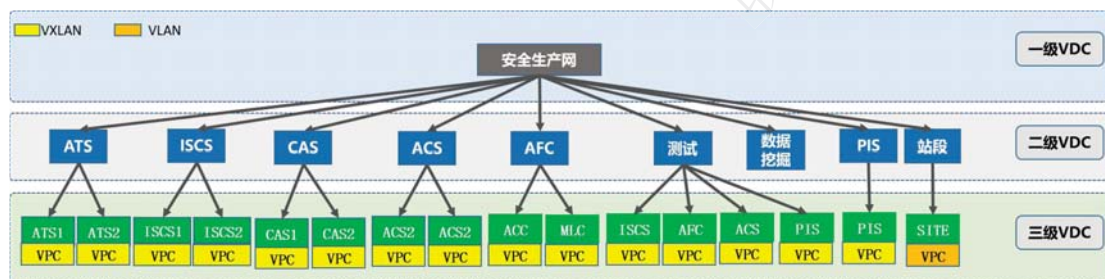
云平台虚拟数据中心（VDC）功能可对应实体部门或逻辑组织等，在平台中表现为租户，实现资源分级管理及组织范围内资源灵活调配。VDC 划分要素为：

- 1) 考虑规范；
- 2) 考虑资源物理隔离性；
- 3) 考虑运营维护管理需求；
- 4) 考虑业务隔离性；
- 5) 考虑业务部署和扩展需求；
- 6) 发挥资源共享优势。

基于建模要素考虑，遵循安全生产网“按专业划分 VDC，按线路划分 VPC”方式，可建立三层 VDC 模型，可灵活适用于业务管理维护需求。内部管理网、和外部服务网设置为一级 VDC，向下可按需灵活分级。

三级 VDC 模型，可实现各业务系统集中管理、分专业管理以及专业内细分线路管理。一级 VDC 管理员可以管理维护二、三级 VDC 内的资源；二级 VDC 的管理员可以管理维护该二级 VDC 下的三级 VDC 内的资源；三级 VDC 管理员只能管理维护自身 VDC 内的资源。同时，管理员可以根据 VDC 粒度做监控、计量、统计、生成报表等。

由于各城轨云平台项目特点各不相同，可按自身需求决定是否配置站段云。呼和浩特城轨云的环境中，在车站部署了安全生产网站段云节点，为 ISCS、AFC、PIS 等专业提供降级模式下所需资源。安全生产网的站段云采用虚拟化方式部署，站段云网络未纳入中心 SDN 网络管理范围内，中心云管理平台对站段云管理能力有限。使用这种方式进行配置时，可为站段云整体设成一个二级 VDC，各站分别设置三级 VDC，站内业务系统可通过网络 VRF 及安全组方式隔离。



三级 VDC 必包含一个 VPC，即云上每条线的业务系统都会拥有自己独立的 VPC 网络。呼和浩特城轨云中，VPC 内可创建内部网络、路由网络和直连网络三种网络类型。内部网络适用于要求完全独立的网络环境，且无需与外部直接通信的业务；路由网络可实现与 VPC 内其他路由网络或外部网络通信，提供弹性 IP 和 SNAT 等服务；直连网络适用于业务系统需要与多种网络通信的场景，自身不包含网络资源，直连网络通过与外部网络相连，在创建虚拟机时实际上使用外部网络 IP，因此此中网络类型要求有全局统一规划 IP。

通过分析呼和浩特城轨云各云上各业务系统网络访问关系，存在 VPC 内互访、VPC 与 VPC 间互访、VPC 与非云网络（外部网络）互访等多种场景，因此，在呼和浩特城轨云中基于全网统一 IP 规划的前提下，各 VPC 内创建直连网络类型，通过三层路由、VPC 关联的防火墙、VPC 内的安全组等多种方式实现业务系统间的互访与隔离的精细控制。

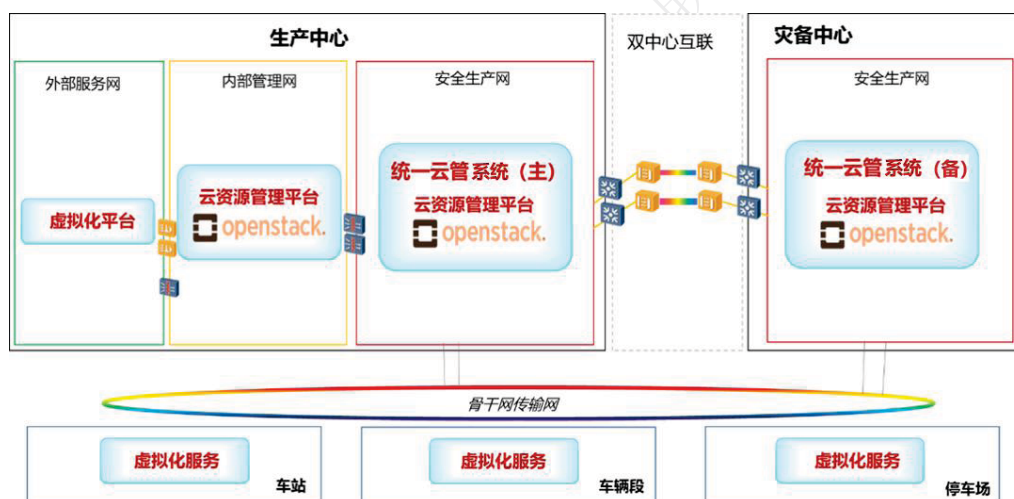
呼和浩特环境使用全局 IP+VPC 内直连网络类型的配置，是在平衡云平台 VDC/VPC 隔离机制和在现有环境下，城轨各系统内或系统间紧密的互联需求后采用的一种方案。以此方式实施，可以有效减少云平台对互访地址的配置和管理工作，会让整体网络的路由规则更简单，对网络故障排查和后续维护也会相对容易。

3.1.3. 城轨云平台管理

3.1.3.1. 云管理系统

城轨云平台的主要基础设施部署在主用中心和灾备中心，同时各个车站、停车场、车辆段部署小规模虚拟化基础设施，通过统一云管理平台对主用中心、灾备中心和站段的云资源进行统一管理，构成线网级城轨云平台。

主备双中心 3 个业务网域均可独立成 Region，均需单独配置云资源管理平台。如果灾备中心配置完整，双中心有 6 个云资源管理平台。统一云管理系统主备中心各部署一套，采用主备模式，主备系统均可管理全平台资源。统一云管理系统可部署在主备中心的运维管理网，也可根据实际需求部署在业务网域内。



呼和浩特城轨云平台共划分了 3 个 Region，也只需要 3 个云资源管理平台，分别是主用中心安全生产网，主用中心内部管理网，灾备中心安全生产网。主备统一云管理系统分别部署在主用中心安全生产网和灾备中心安全生产网，当主用中心统一云管理系统宕机后，只要业务网络可达，灾备中心同样可对全平台进行管理。主用中心系统恢复后可手动切换。主用中心外部服务网使用虚拟化平台，通过独立云管通道接入统一云管理系统。

实际部署软件和部署架构包括：

1) 统一云管理系统

云管理系统提供统一的城轨云运营管理和运维管理功能，除了资源管理之外，统一云管理系统除了资源管理外，还会对 SDN 网络和安全资源进行统一管理和联动。在主用中心和灾备中心以“主-备”模式部署，并可以实现对主用中心外部服务网、车站/车辆段/停车场部署的虚拟化资源进行统一管理，统一云管理平台可与安全生产网云资源管理平台合并部署。

2) 云资源管理平台

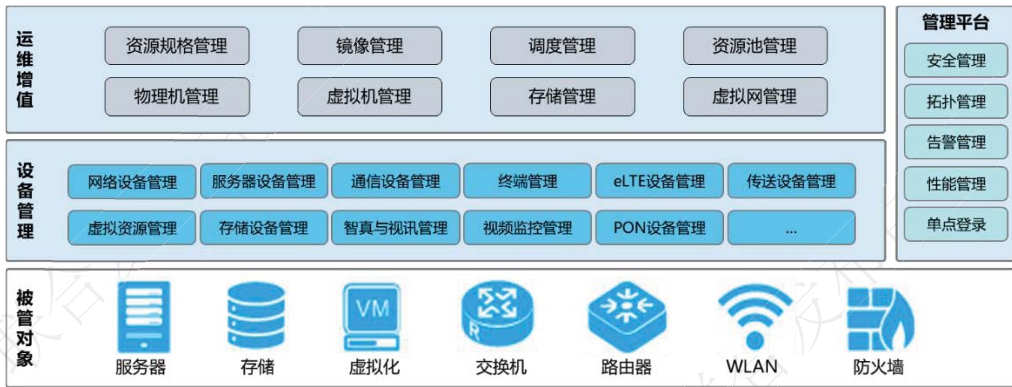
提供云平台内完整的计算资源、存储资源和网络资源等基础资源的管理服务。计算、网络、存储等资源被 OpenStack 集成和服务化之后，再被上层的统一云管理平台进行管理。同时 OpenStack 负责收集虚拟资源池的告警、性能、资源等监控数据，并汇聚上报到云管理平台进行统一呈现。

3) 虚拟化平台

基于 KVM 的虚拟化平台，为服务器提供基本的虚拟化能力，在呼和浩特城轨云平台中，主用中心的外部服务网和各车站/车辆段/停车场部署虚拟化平台，为部署在主用中心外部服务网和各车站/车辆段/停车场的上云业务应用提供虚拟化环境，同时虚拟化平台会通过北向接口直接被统一云管理平台所管理。

3.1.3.2. 系统管理（网管）

城轨云平台作为线网级综合云平台，应遵循“一网覆盖”的理念，通过运维管理网统一将服务器、网络设备、安全设备、存储设备进行管理。系统平台应提供对云平台设备的网元级管理的同时，提供丰富的维护辅助功能及准确的监控告警功能，帮助运维人员基于一个平台维护全网设备，有效降低运维成本及人员压力，提高维护自动化、智能化水平。



城轨云系统管理平台的基础功能包含统一的网络和设备管理。平台逻辑架构包括：管理平台、设备管理组件和运维增值组件三部分：

1) 管理平台

提供安全管理、拓扑管理、告警管理、性能管理、单点登录等基础管理功能，提供网管自身的维护工具和系统监控。

2) 设备管理组件

支持对网络设备、存储设备、服务器等进行批量配置，有效提高运维效率，降低运维成本。

3) 运维增值组件

提供部署、监控、诊断和分析工具，实现业务快速开通、问题主动预防、故障准确定位等功能，保障城轨云平台系统稳定运行。

城轨云的基础管理功能就是以上提到的资源管理和设备管理两部分。在这个基础之上，协会提出，云平台管理需要有 3 个中心：云管中心、运维中心、安全管理中心。这 3 个中心的功能分别如下：

1) 云管中心

既有云管理平台和网管平台的综合。

2) 运维中心

运维中心依赖于云管中心的集中监管能力，基础功能包括能监控全网的设备实时状态、集中收集并处理告警信息、管理备品备件和流转维护工单等。运维中心有部分定制化的要求，需根据实际运维需求和流程进行定制化开发，建议系统能提供符合 ITIL 规范的服务功能。

3) 安全管理中心

即网络安全等级保护中所要求的安全管理中心，要能对全网的安全设备集中管控，能对审计数据汇总并集中分析，能对安全策略、安全补丁等安全相关事项进行集中管理，能对各类安全事件进行识别、报警和分析。

3.1.4. 功能及服务

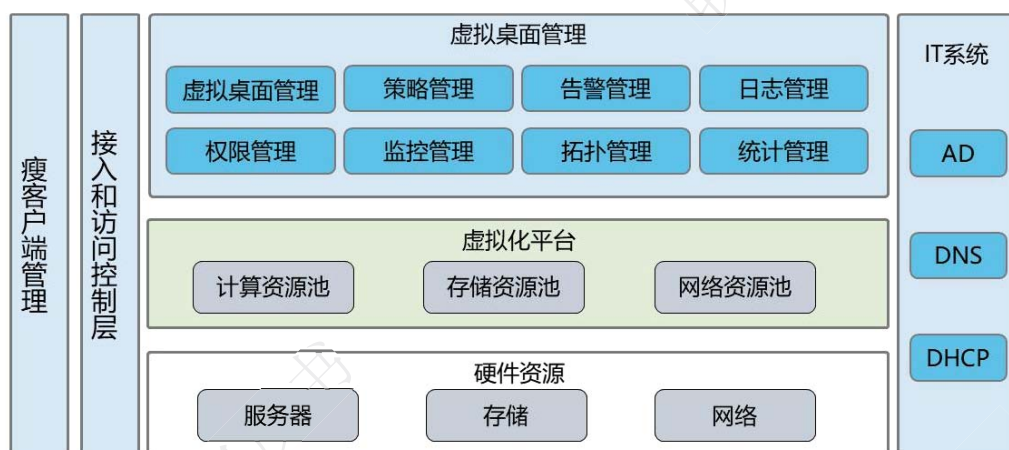
3.1.4.1. 桌面云

桌面云服务以服务器虚拟化为基础，允许多个用户桌面以虚拟机的形式独立运行，同时共享 CPU、内存、网络连接和存储器等底层物理硬件资源。通过将虚拟机彼此隔离实现精确的资源分配，并能保护用户免受由其他用户活动所造成的应用程序崩溃和操作系统故障所带来的影响。

桌面云提供与 PC 一致的桌面体验，用户可以灵活访问与普通 PC 桌面功能相同的个性化虚拟桌面，简化桌面的管理、调配和部署。桌面云在虚拟机开机、关机过程中，用户可完整看到虚拟机开机和关机过程，提供类似于 PC 一样的体验。用户可以安全方便地访问虚拟桌面，将数据、信息和知识财产保留在企业内部。

为了系统安全性，桌面云系统具备用户身份认证功能和权限管理功能，对应不同的应用层次。既能保证不同用户高效、快速地访问控制授权范围内的系统资源，也能有效地阻止用户之间的非法侵入、非授权访问，并且能提供统一的操作日志查询和审计功能，包括桌面云运行维护操作日志、虚拟化平台运行维护操作日志、硬件管理运行维护操作日志。桌面云管理系统中的账号所属角色对应的操作权限需进行分离，要求将业务管控、系统配置、日志管理、告警管理和账号角色管理等操作内容进行分离，不允许同一类角色有全部的权限，进而增强系统账号的安全性。

桌面云系统的逻辑架构图如下：



1) 硬件资源

提供部署桌面云系统相关的硬件基础设施，包括服务器、存储设备、网络设备等。

2) 虚拟化平台

根据虚拟桌面对资源的需求，把桌面云中各种物理资源虚拟化成多种虚拟资源的过程。包括计算虚拟化、存储虚拟化和网络虚拟化。

3) 虚拟桌面管理层

负责对虚拟桌面使用者的权限进行认证，保证虚拟桌面的使用安全，并对系统中所有虚拟桌面的会话进行管理。

4) 接入和访问控制层

用于对终端的接入访问进行有效控制，包括接入网关、负载均衡器等设备。

5) 瘦客户端

用于访问虚拟桌面的特定的终端设备。

3.1.4.2. 关键云服务

本节所列的云服务主要是针对 IaaS 层，包括计算、存储、网络、容灾等底层服务。这些服务基本覆盖了业务系统在城轨云上部署的所需。呼和浩特城轨云平台完全覆盖了这个层面的服务。

针对 PaaS 层服务，云平台能提供的类型会更加多样，如中间件服务、数据服务、容器服务和分析服务等。以上服务可以由云平台厂商提供，也可以由业务系统依照接口标准提供。PaaS 层提供的服务取决于业务系统的需求，以及对未来新的智能应用的规划。

1) 计算服务

- 弹性云服务器

提供一种可随时自助获取、可弹性伸缩的云服务器，帮助使用者打造可靠、安全、灵活、高效的应用环境，确保服务持久稳定运行，提升运维效率。

支持指定云服务器类型和规格创建云主机，支持根据预制的多种类型云服务器可供选择，针对不同的应用场景，可以选择不同规格的弹性云服务器。

- 裸金属服务器

为应用提供专属的物理服务器，提供卓越的计算性能，满足核心应用对高性能及稳定性的需求，结合了传统物理服务器的稳定性与云中资源高度弹性的优势。

支持将物理服务器定义成服务目录供用户选择和使用，用户可以根据自己的需要选择物理机镜像，并且能够实现自动化完成卷挂载、安装软件和网络配置等工作。

- 镜像服务

提供镜像服务，可为弹性云服务器实例提供可选择的运行环境模板，运行环境模板一般包括操作系统和预装的软件。通过镜像服务，可以实现弹性云服务器实例的快速部署。镜像包括公有镜像、私有镜像。

镜像服务支持私有镜像在云服务可用区内共享，支持使用者可以在创建弹性云服务器实例时选择私有镜像，支持使用者可以在创建弹性云服务器实例时选择被共享镜像。

2) 存储服务

- 云硬盘服务

提供弹性扩展的虚拟块存储服务。像使用传统服务器硬盘一样，使用者可以对挂载到云服务器上的云硬盘做格式化、创建文件系统等操作，并对数据做持久化存储。

3) 网络服务

- 虚拟私有云（VPC）服务

提供虚拟私有云服务，用于帮助使用者在云中虚拟出一个私有的应用运行环境和安全域。VPC 能够提供安全、隔离的网络环境，为应用或虚拟机提供网络资源，实现应用向云上的平滑迁移。

云平台也可为 VPC 内不同网络间或不同 VPC 间互通提供三层通信转发配置，用于 VPC 内不同网络间，及 VPC 内的子网与外部网络的连接配置，为虚拟机提供三层通信转发能力，并保证 VPC 的三层隔离功能。

- 弹性 IP 服务

平台提供弹性 IP 服务，用户可将获得的公网 IP 地址与租户 VPC 内部署的弹性云服务器的内部 IP 地址进行映射，从而实现外部用户对该应用的访问，提供弹性 IP 服务的自助申请。弹性 IP 支持自助绑定、解绑弹性云服务器的 IP 地址。

- 虚拟防火墙服务

虚拟防火墙通过在核心交换机旁挂实体防火墙，再由实体防火墙虚拟出虚拟防火墙和云管理平台联动后的产物，将安全作为一项服务对业务人员呈现。虚拟防火墙本质上是对 VPC 的访问控制策略系统，根据与 VPC 关联的入站/出站规则，判断数据包是否被允许流入/流出关联 VPC。

- 安全组服务

安全组是一个逻辑上的分组，为同一个 VPC 内具有相同安全保护需求并相互信任的弹性云服务器或裸金属服务器提供访问策略。安全组创建后，可以在安全组中定义各种访问规则，当服务器加入该安全组后，即受到这些访问规则的保护。默认安全组的规则是对出方向上的数据报文全部放行，入方向访问受限，安全组内的服务器无需添加规则即可互相访问。一个服务器可以加入多个安全组，且与每个安全组内的服务器都可以互相访问。

安全组与虚拟防火墙工作的层面不同。防火墙工作于路由器端口，控制进出网络的数据流。安全组则工作于虚拟机端口，对指定虚拟机的数据流进行控制。

4) 容灾服务

- 云服务器容灾服务

云服务器容灾服务为云服务器提供跨中心的容灾保护。当主用中心发生灾难时，可在容灾中心恢复受保护的云服务器。

- 云硬盘高可用服务

云硬盘高可用服务为云服务器中的云硬盘提供本地存储双活保护。当单套存储设备发生故障时，数据零丢失，业务不中断。

3.1.5. 业务降级及线路扩展

3.1.5.1. 业务系统的降级运行

降级运行通常是指城轨系统由于设备故障或其他原因不能按照系统设计目标运作，而只能在一个较低的水平上（即降级）运行。产生降级运行的情况和场景有很多，典型的如信号系统的自动驾驶模式（ATO 模式），在设备故障时采用人工模式驾驶，就是降级运行。

当使用城轨云平台承载业务系统时，云平台同样存在故障的可能性，城轨云平台具有主用中心与灾备中心的双中心结构，各线路站段和两中心间需均有网络连接。在应用支持的情况下，如果主用中心系统宕机，可切换至灾备中心继续操作。这部分属于城轨云灾备及备份功能，后面有专门章节进行论述。业务系统可在双中心均不可用的情况下实施降级运行，进行站级控制或人工控制。比起传统的部署方式，城轨云平台能够提供更多的冗余与灾备能力，但需要应用系统针对城轨云的环境做相应适配。

呼和浩特城轨云对业务系统容灾及降级运行的设计如下：

- 1) 信号（ATS）系统：中心 ATS 应用双活，在灾备中心有应用系统部署。站级 ATS 不上云，降级模式下进行站控。
- 2) 综合监控（ISCS）系统：中心 ISCS 系统数据双活。站段云上部署综合监控后备服务器，在站段的控制终端实施 1+1 配置，即 1 个云桌面终端、1 个物理终端。
- 3) 自动售检票（AFC）系统：中心数据双活，站段云上部署自动售检票系统站机（SC）的后备服务器，用于实现闸机紧急放行等操作。当发生中心故障时，票款信息会暂存在设备内，等恢复后再同步到中心。站段的控制终端实施 1+1 配置。呼和浩特地铁 AFC 系统弱化了站机（SC）层，其它城市实施时需根据实际情况确定站段云承载的 AFC 应用与功能。
- 4) 乘客信息（PIS）系统：中心数据双活，站段云上部署乘客信息后备服务器，用于实现在降级模式下的火警告警等功能，可与自动售检票闸机紧急放行功能配合使用。站段的控制终端实施 1+1 配置。

3.1.5.2.对未来线路的扩展与预留

城轨云平台承载的是多线路的业务系统，平台的规模会随着承载线路的增加而逐步扩大。因为云平台具有平滑扩展的特性，初始平台规模仅满足当期需求即可。

建议在初始平台设计时，应根据最终的规划考虑足量的机房空间、供电与散热、线路接入能力（如成端端口、配线架等）、网络能力，这些资源在后期升级时相对困难。而计算能力、存储能力的升级则较为简单，只需按需增加相应资源即可，可以支持在线扩容。安全防护建议选择有扩展能力的设备或系统。

新建线路要接入既有城轨云平台，云平台所需要的扩容工作包括：

- 1) 增加新线路中心系统所需计算资源和存储功能
- 2) 增加新线路系统所需的云桌面资源
- 3) 新增站段云所需资源和设备
- 4) （如需要）增加相应的软件授权。

3.2. 网络设计

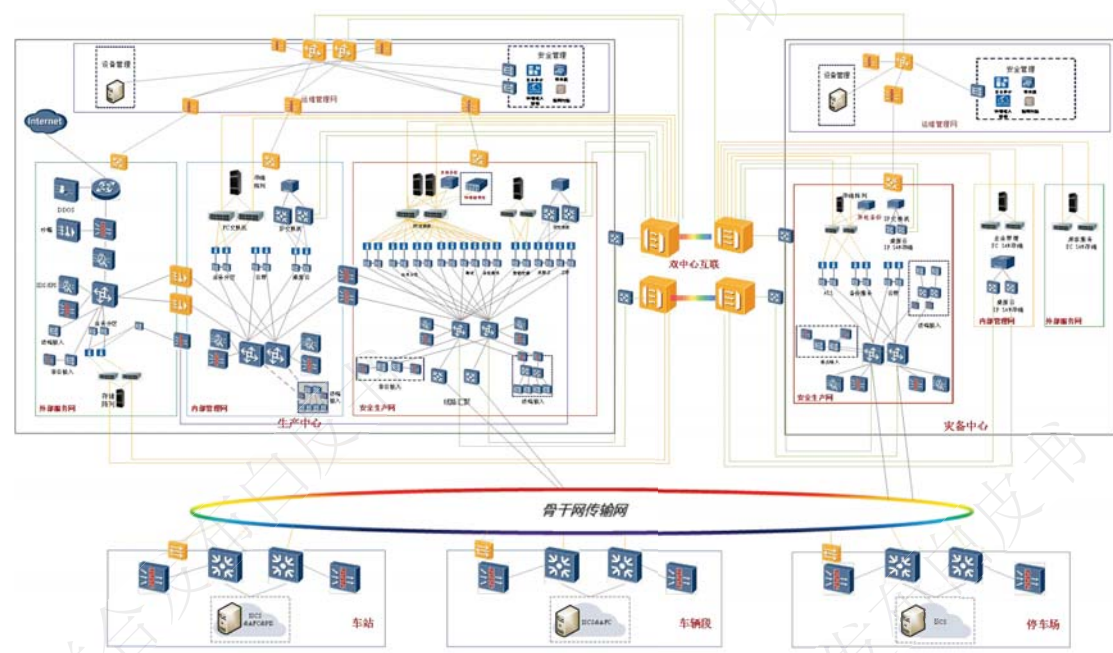
随着城市轨道交通的高速发展，各城市建设线路不断增多，作为承载多线路的综合云平台，城轨云平台需具备极强的扩展性及灵活性。传统数据中心在组网方面能力不足越来越明显，主要体现在：网络虚拟化的支持能力不足，不支持业务自动化部署和灵活编排。通过引入 SDN 网络解决方案，基于集中控制、业务与控制分层的架构实现网络资源全局集中管控、智能调度，并且通过与云平台对接，实现业务网络自动化部署和灵活编排，同时对新建线路有很好的扩展性，极大的简化了新建线路组网配置。

3.2.1. 网络整体架构

城轨云网络架构按物理划分，由线网中心网络、通信传输网络、站段局域网、车地无线通信网络、车载网络五部分组成，按照应用、管理及安全防护等级的不同，分为安全生产网、内部管理网、外部服务网业务网络以及运维管理网。灾备中心做为主中心的备份站点，对应部署安全生产网、内部管理网、外部服务网以及运维管理网。由于灾备中心内部管理网、外部服务网区域无计算资源，故灾备中心内部管理网、外部服务网只部署了存储相关网络。

车站、车辆段、停车场均部署站段业务网络，接入站段各个业务系统。各个站段网络上行通过骨干传输网络和生产、灾备数据中心安全生产网互联，实现站段和中心的数据交换。每个车站、车辆段、停车场均部署 1 台带外管理交换机，带外管理交换机上行通过骨干传输网分别接入到生产、灾备中心运维管理网。主中心管理网、灾备中心管理网、站段管理接入交换机共同组成城轨云运维管理网。

呼和浩特城轨云方案由于实际条件有一定限制，如外部服务网使用了单核心配置。后续城轨云建设可参考呼和浩特的方案，根据实际需求进行调整。



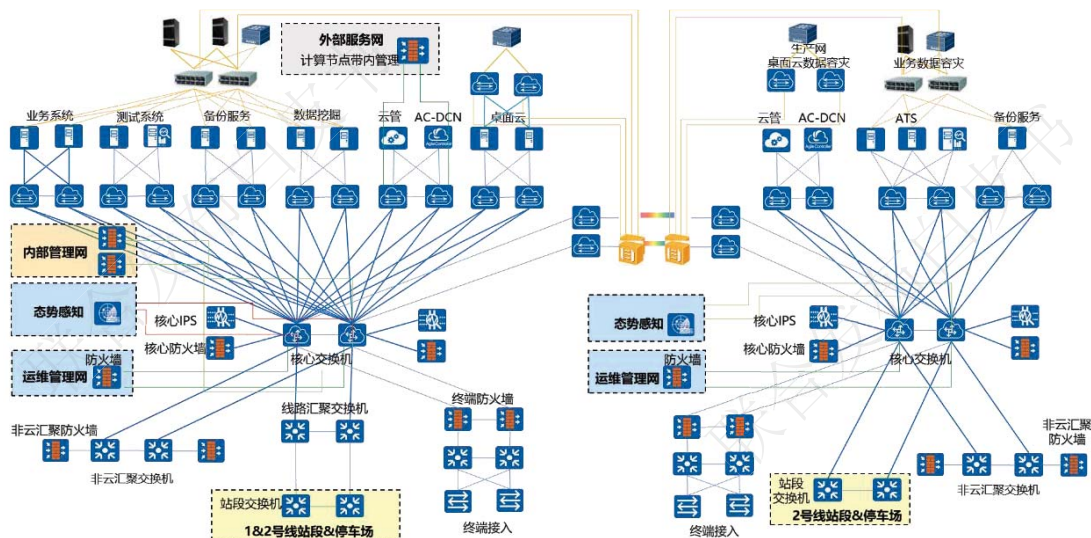
城轨云采用中心级和车站级进行部署，主用中心和灾备中心在网络层通过线网骨干传输实现网络同步。线路骨干传输网组建以 OCC 和车辆段为相交点的环网。线路骨干传输设备采用 40G 的增强型 MSTP 设备，支持物理硬管道做业务的物理隔离。

线网承载网随线路增加带宽递增，采用 MS-OTN 组建一个线网承载环网，承载网带宽支持 100G、200G、400G 大流量承载。按线路增加线网承载网节点，对接线路车辆段传输设备。车辆段到灾备中心通信，通过线网承载环网节点传输数据到灾备中心的传输节点。

主用中心和灾备中心之间通过骨干 MS-OTN 节点对接传输数据。

3.2.2. 安全生产网

3.2.2.1. 安全生产网组网



主中心安全生产网核心部署 2 台核心交换机（Spine 节点），核心交换机旁挂 2 台核心防火墙，用于东西向及南北向安全控制。核心交换机还会旁挂 2 台核心 IPS，用于入侵检测防御。主中心安全生产网接入部署多台业务接入交换机（Leaf 节点），分别用作业务系统、备份服务、数据挖掘、云管、桌面云的业务接入。主中心部署 1 套 CIS（态势感知）系统，对流经核心交换机的数据流进行镜像分析，展示网络安全态势。

部署 2 台边界防火墙，做为和内部管理网之间区隔的网络边界隔离和防护设备。

针对各个业务系统的非上云设备（云下设备）及传统不上云业务系统，主中心部署 2 台非云接入交换机和 2 台非云边界防火墙，用于云下设备及非云系统的汇聚接入。

在主中心安全生产网部署 2 台线路汇聚交换机，用于 1、2 号线站段及停车场网络的汇聚接入，同时可用于未来 3、4、5 号线的汇聚接入。

主中心部署 2 台终端汇聚交换机、2 台边界防火墙用于终端系统的汇聚和安全防护，部署 10 台终端接入交换机（分布在各楼层），用于桌面云系统的终端接入。

在呼和浩特城轨云的实践中，云管理系统部署在安全生产网，外部服务网并没有部署云管理系统，其虚拟化系统由部署在主中心安全生产网的云管理系统统一纳管，外部服务网虚拟化系统管理平面通过外部服务网管理边界防火墙，接入主中心安全生产网核心交换机。考虑到安全生产网和内部管理网内的云管流量是和业务流量在一个网络平面上，外部服务网的云管通道采用直接在业务网络内打通的方式，而不是从运维管理网绕行。

灾备中心安全生产网核心部署 2 台核心交换机（Spine 节点），核心交换机旁挂 2 台核心

防火墙，用于东西向及南北向安全控制。核心交换机还会旁挂 2 台核心 IPS，用于入侵检测防御。灾备中心接入部署多台业务接入交换机（Leaf 节点），分别用作业务系统、备份服务、云管的业务接入。灾备中心部署 1 套态势感知系统，对流经核心交换机的数据流进行镜像分析，展示网络安全态势。

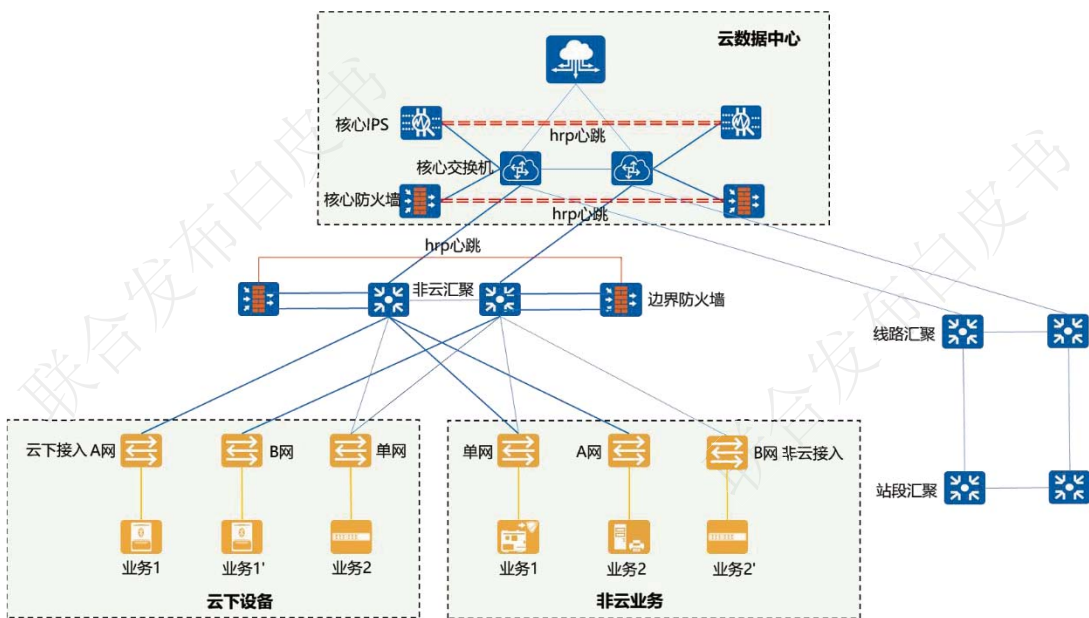
灾备中心部署 2 台非云接入交换机和 2 台非云边界防火墙，用于云下设备及非云系统的汇聚接入。2 台终端汇聚交换机、2 台边界防火墙用于终端系统的汇聚和安全防护，部署 2 台接入交换机，用于桌面云系统的终端接入。

在呼和浩特的实际部署中，1、2 号线站段及停车场汇聚交换机上行接入骨干传输网，1、2 号线传输网在主中心接入云平台线路汇聚交换机，2 号线传输网在灾备中心接入云平台灾备核心交换机，实现站段及停车场对主、灾备数据中心的访问。在后续线路建设时，灾备中心可参考主中心配置，增加云平台的线路接入交换机，并接入所有线路的传输网。

由于日志分析、漏洞扫描、终端准入控制系统等安全系统均部署在运维管理网，需要打通安全生产网和运维管理网网络通道。通过主中心安全生产网核心交换机和灾备中心核心交换机，分别和运维管理网主中心安全生产网管理分区边界防火墙和灾备中心管理分区边界防火墙互联，实现安全可控的互访。

主中心和灾备中心各部署 2 台互联交换机，通过波分系统互联。实现安全生产网主备数据中心的数据交互。

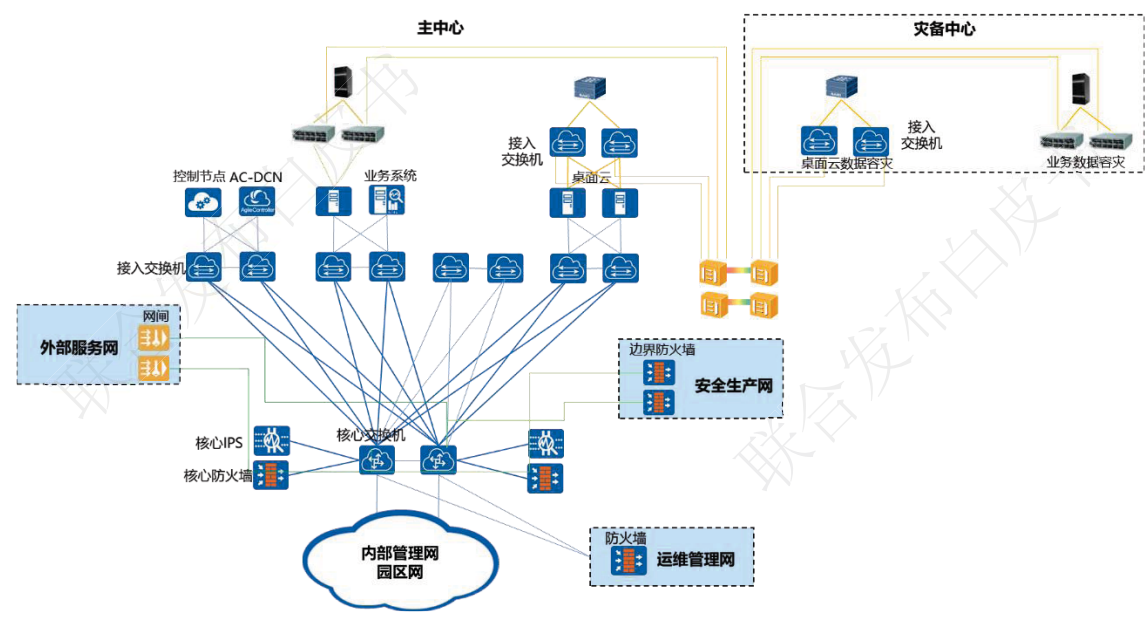
3.2.2.2.非云业务接入组网



安全生产网主备中心各部署 2 台非云接入交换机，做为云下设备及非云业务的汇聚，2 台交换机独立部署，和数据中心核心交换机形成口字型组网。旁挂边界防火墙，用于云下设备及非云业务的安全防护。

云下设备及非云业务有 2 种接入方式。如果是 A、B 网接入，则有 2 台业务接入交换机（A/B），A 网交换机和 B 网交换机上行分别和 1 台非云接入交换机互联；如果业务系统是单网接入，此交换机上行 2 条链路分别和 2 台非云接入交换机互联，如上图所示。

3.2.3. 内部管理网



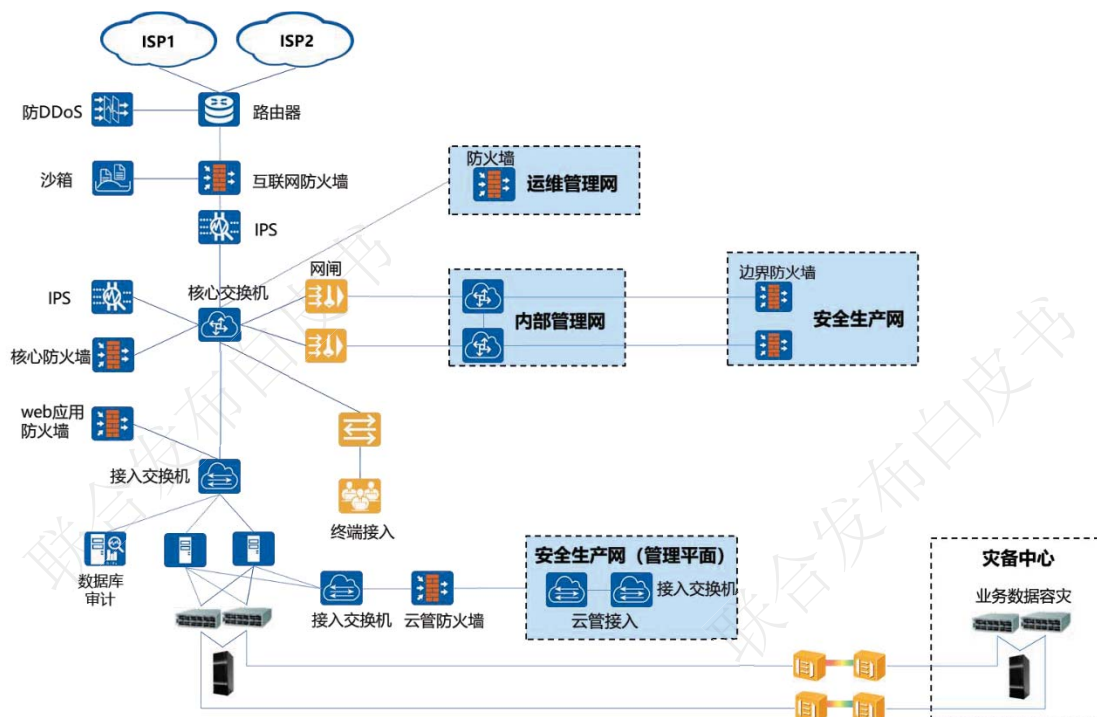
内部管理网主中心核心部署 2 台核心交换机。旁挂 2 台核心防火墙，用于东西向及南北向安全控制，同时旁挂 2 台核心入侵检测防御，用于入侵检测防御。内部管理网接入部署多台业务交换机，分别用作业务系统、云管、桌面云的业务接入。

由于日志分析、漏洞扫描、终端准入控制系统等安全系统均部署在运维管理网，需要打通内部管理网和运维管理网的网络通道。通过内部管理网核心交换机和运维管理网内部管理网管理分区边界防火墙互联，实现安全可控的互访。

内部管理网对外通过 2 台网闸和外部服务网互联，对内通过 2 台边界防火墙和安全生产网互联。为了数据的高可靠，针对业务系统和桌面云数据在灾备中心部署了数据容灾系统。主备双中心的内部管理网通过波分系统互联，实现数据灾备。

呼和浩特城轨云平台内部管理网并没有部署站段云节点（站段云汇聚交换机）。所有内部管理网涉及的终端网络，在中心汇聚后直接接入内部管理网核心交换机。建议后续城轨云可包括内部管理网至站段层的终端网络，便于整体运维。

3.2.4. 外部服务网



外部服务网没有采用 OpenStack+SDN 的配置，而是采用虚拟化+传统网络配置。主中心核心部署 1 台核心交换机，旁挂 1 台核心防火墙，用于东西向及南北向安全控制，同时旁挂 1 台核心 IPS，用于入侵检测防御。外部服务网接入部署多台业务接入交换机，其中 2 台用于业务系统接入，1 台用于接入云管理平台。

外部服务网出口部署 1 台出口路由器，用于和电信运营商互联，实现互联网用户访问城轨云服务。出口路由器旁挂 1 套防攻击系统，阻止来自互联网的 DDoS 攻击。

出口路由器和核心交换机之间以此串接 1 台边界防火墙和 1 台边界 IPS 设备，边界防火墙旁挂 1 台沙箱设备，实现互联网未知安全威胁（APT）的检测和阻断，同时，根据业务需要，在边界防火墙上做 NAT，实现内网到公网的地址映射。边界 IPS 用于入侵防御，阻止外网的非法入侵。

在外部服务网核心交换机和业务接入交换机之间串接 1 台 WAF 安全设备，采用透明代理的方式部署，用于外部服务网 WEB 安全防护。

由于日志分析、漏洞扫描、终端准入控制系统等安全系统均部署在运维管理网，需要打通外部服务网和运维管理网网络通道。通过外部服务网核心交换机和运维管理网外部服务网管理分区边界防火墙互联，实现安全可控的互访。

核心交换机通过 2 台网闸和内部管理网互联，实现安全可控的数据交互。由于外部服务网虚拟化系统由部署在安全生产网的云管理系统统一纳管，外部服务网虚拟化系统管理平面通过云管接入交换机，经过管理边界防火墙，接入安全生产网核心交换机。

呼和浩特城轨云平台外部服务网并没有部署站段云节点（站段云汇聚交换机）。因为呼和浩特 CCTV 并未纳入云平台，PBE 是汇聚到中心后再通过外部服务网非云接入交换机接入云平台。建议后续城轨云建设可部署外部服务网的站段云系统，使整个结构更符合《规范》要求。

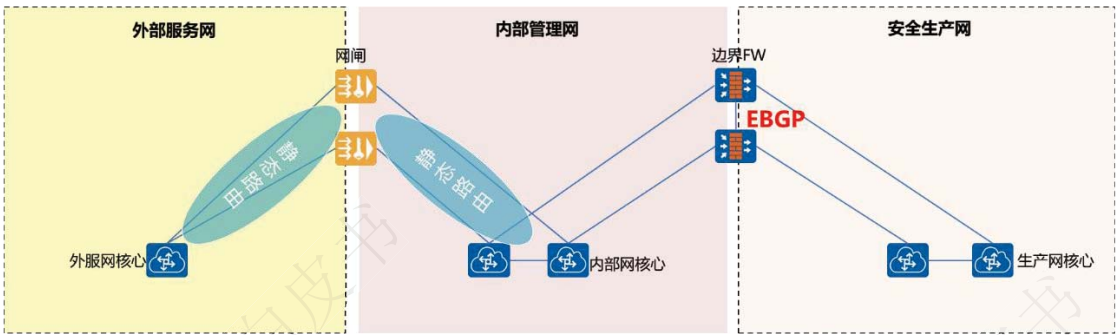
3.2.5. 三网横向流量

城轨云三个业务网域承载不同安全等级的业务系统，业务之间大量交互在同网域内完成。同时，随着业务功能不断多元化，跨网域间通信不可避免，在此情况下，需要在网域间设置不同的安全防护措施实现网域间精确、安全通信。

安全生产网与内部管理网之间通过业务边界防火墙进行路由级别隔离，边界防火墙运行在透明模式；安全生产网核心交换机和内部管理网核心交换机之间均运行 EBGp，只发布需要互访的网段路由。

内部管理网与外部服务网之间通过信息安全交换系统（简称网闸）实现内外网物理级别隔离。内部管理网、外部服务网到网闸均配置静态路由。

业务在三网之间的数据流量在网域间边界设备防护基础上，仍有 IPS、VPC 关联的防火墙、安全组等多重防护。

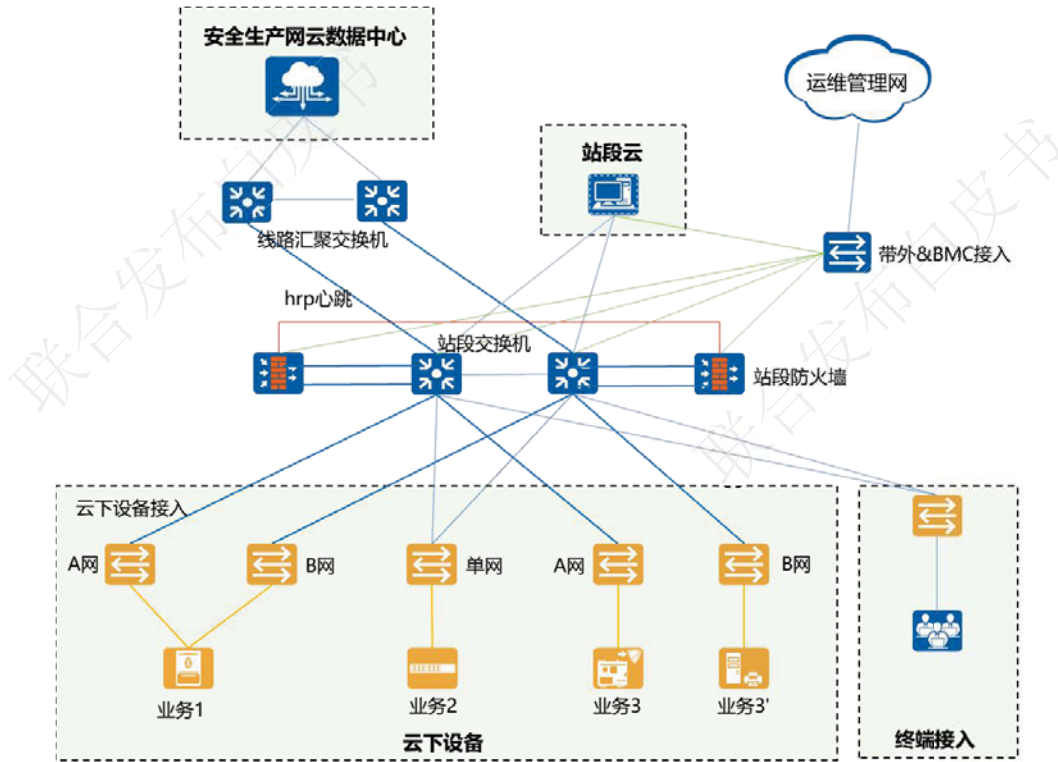


三网之间访问关系：

业务系统	数据路径	说明
数据挖掘	安全生产网->内部管理网	安全生产网单向将结果数据推送至内部管理网数据挖掘关系型数据库
数据挖掘	内部管理网<->外部服务网<->互联网	获取互联网节假日信息，以及手机 APP 支持
企业信息化	内部管理网->外部服务网	邮箱、公司网站等
综合监控-CCTV	外部服务网<->内部管理网<->安全生产网	综合监控和 CCTV 联动
AFC	外部服务网<->内部管理网<->安全生产网	APP 售票子系统访问 ACC\MLC 后台

		及加密机等
PBE-CAS	外部服务网<->内部管理网<->安全生产网	PBE 工作站与集中告警通信

3.2.6. 站场段网络



站段云作为中心云平台的延伸，完整架构下应同样保持安全生产网、内部管理网、外部服务网的 3 网域架构。呼和浩特城轨云仅部署了安全生产网部分，即所有站段及停车场部署 2 台安全生产网站段云汇聚交换机，用于站段云接入和各业务系统在站段云下设备的汇聚。2 台交换机独立部署，上行和线路汇聚交换机形成口字型组网架构。旁挂边界防火墙，对各业务系统站段云和云下各系统进行安全隔离和防护。

站段及停车场各业务系统云下设备，如果是 A、B 网接入，则有 2 台接入交换机（A/B），业务 A 网交换机和业务 B 网交换机分别和 1 台站段云汇聚交换机互联；如果业务系统是单网接入，则只有 1 台业务交换机接入，此交换机上行分别和 2 台站段云汇聚交换机互联。

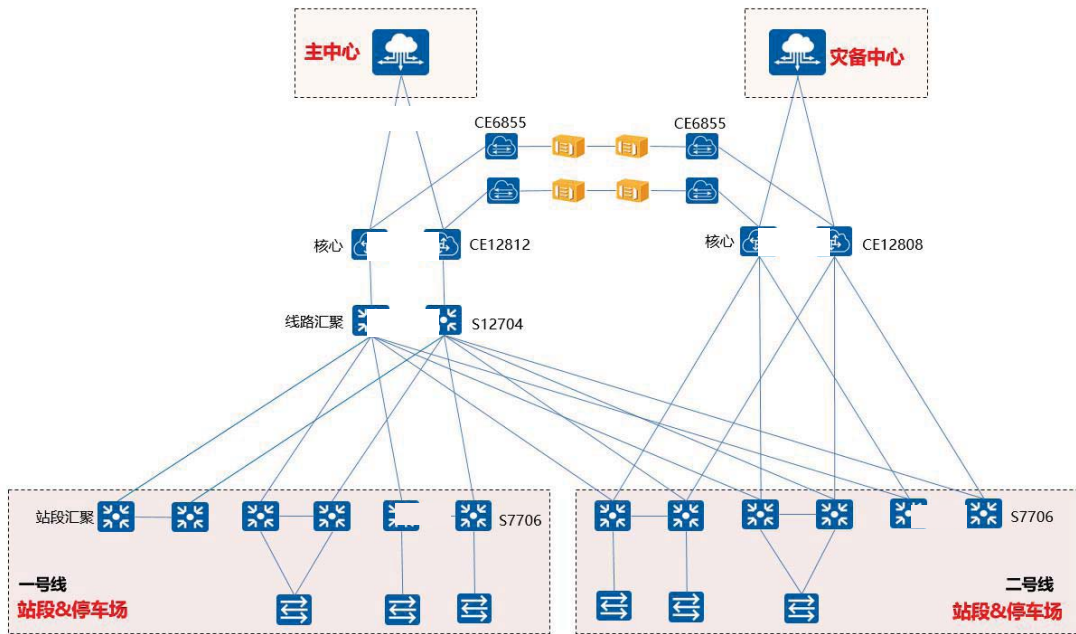
各个站段及停车场都配置了一些终端设备。对于安装位置离机房比较近（小于 100m）的终端，终端直接使用 RJ45 接入站段云汇聚交换机。对于安装位置比较远（大于 100m）的终端，终端先接入到 1 台远端终端接入交换机，再使用光纤上联接到站段云汇聚交换机。

每个站段及停车场部署一台站段云带外管理交换机，用于站段及停车场网络设备和站段云服务器的管理接入。上行接到运维管理网安全生产网管理分区汇聚交换机。

在呼和浩特城轨云实践中，车站、停车场、车辆段的配置都一样，都只是部署了安全生

产网站段云节点。因车辆段有大量的办公需求，办公网络是基本要求。在后续的城轨云建设中，建议车辆段的站段云应至少包括安全生产网和内部管理网这两个网域。

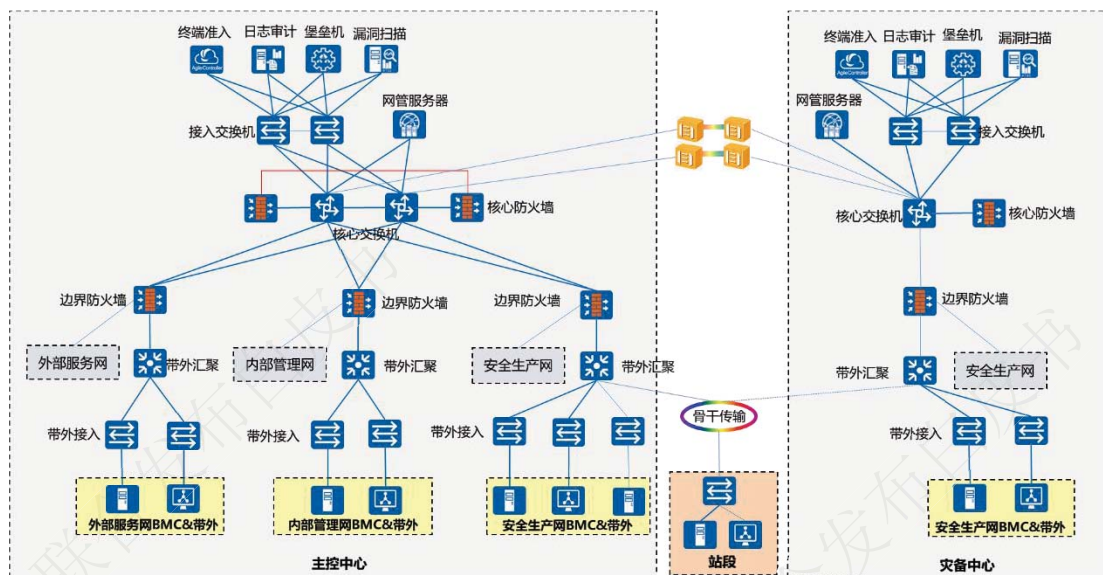
3.2.7. 双中心网络



呼和浩特城轨云双中心互联网由主中心核心交换机、主中心线路汇聚交换机、主备中心互联交换机、灾备中心核心交换机及 1、2 号线站段及停车场站段汇聚交换机组成。区别于数据中心各个业务网，城轨云双中心互联网承载了站段及停车场和数据中心以及主备数据中心之间的数据交互。

呼和浩特城轨云双中心网全网采用口字型组网架构，包括：主中心核心交换机和线路汇聚交换机、和站段及停车场汇聚交换机、主中心核心交换机和灾备中心核心交换机，及灾备中心核心交换机和站段及停车场站段云汇聚交换机之间互联，均采用了口字型组网架构。

3.2.8. 运维管理网



运维管理网主中心核心部署 2 台运维核心交换机，2 台设备堆叠部署，以提高设备可靠性。运维核心交换机旁挂 2 台核心防火墙，用于安全系统及网管系统的安全防护。运维管理网各安全系统通过接入交换机接入，网管直接接入运维核心交换机。运维管理网主中心设置三个分区，分别是安全生产网管理分区、内部管理网管理分区、外部服务网管理分区。三个管理分区每个分区汇聚部署 1 台汇聚交换机，及若干台接入交换机（根据各个分区被管理设备数量灵活调整）。各个管理分区通过边界防火墙和管理核心交换机互联。

运维管理网灾备中心核心部署 1 台核心交换机，旁挂 1 台核心防火墙，用于安全系统及网管系统的安全防护。运维管理网各安全系统通过接入交换机接入，网管系统直接接入运维核心交换机。灾备中心只有安全生产网有计算资源，灾备中心只设置一个分区，为安全生产网管理分区。灾备中心安全生产网管理分区汇聚部署 1 台汇聚交换机，及若干台接入交换机（根据被管理的设备数量灵活调整）。安全生产网管理分区通过边界防火墙和管理核心交换机互联。

各个站段及停车场站段云带外管理交换机上行通过骨干传输网，分别与运维管理网主中心安全生产网管理分区汇聚交换机和灾备中心安全生产网管理分区汇聚交换机相连。

运维管理主中心和灾备中心核心交换机通过波分系统互联，组建统一的运维管理网络。

由于日志分析、漏洞扫描、终端准入控制系统等安全系统需要访问业务网络，需要打通运维管理网和各业务网网络通道。各个业务网核心交换机和运维管理网各管理分区边界防火墙互联，以实现安全可控的互访。

3.2.9. 其它网络

一张完整的城轨云应包含 5 部分：线网中心网络、通信传输网络、站段局域网、车地无

线通信网络和车载网络。整体架构覆盖了城轨系统的中心-车站-列车的“云-边-端”3层。从呼和浩特实践来看，这5部分网络并不全是在城轨云的项目范围内，只有这5部分做到互联互通，才能真正让城轨云平台动起来。

前面章节谈到的安全生产网、内部管理网、外部服务网、运维管理网都属于线网中心网络，站场段网络属于站段局域网，通信传输网络包含2部分，一部分是双中心互联的网络，另一部分是各线路中心-站段间的骨干传输环网。

之前章节未包含的两张网：

- 1) 车地无线通信网：呼和浩特城轨的部署方案是，信号CBTC控制消息采用LTE-M网络传输。车载PIS/车载CCTV流量采用WLAN网络传输。其中车辆运行维护信息也会通过WLAN传至地面。
- 2) LTE-M传输是属于信号ATC网络的一部分，与城轨云并无直接关联。车地间使用WLAN传输的PIS/CCTV/车辆运行维护信息，在地面通过业务系统交换机、站段云汇聚交换机上传至中心。
- 3) 车载网络：车内用于传输车载PIS和车载CCTV流量的网络，多由车载PIS厂商提供。

3.3. 资源设计

3.3.1. 计算资源

1. 设计原则

- 选型统一，便于动态分配

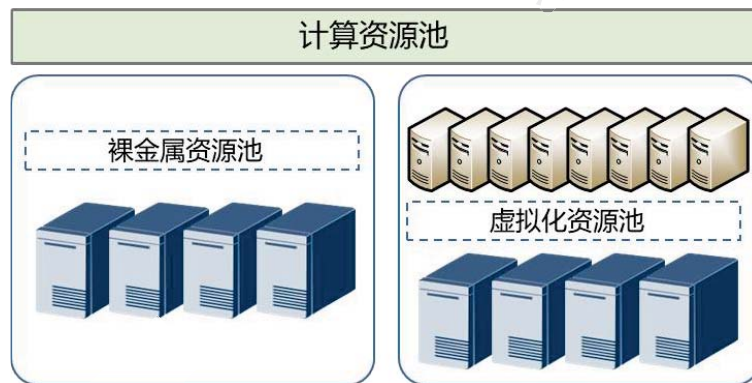
城轨云承载业务众多，各业务对底层服务器计算性能、IO吞吐能力要求各不相同。高低端服务器在性能上差异较大，对于新建城轨云平台建议服务器采用统一档次、统一类型的x86高端服务器，形成虚拟化资源池，便于进行资源动态分配。

- 合理配置，适配业务需求

城轨云平台中应配置虚拟机的同时，可能还需要配置裸金属服务器。裸金属服务器用于无法使用虚拟机或要求独占硬件的业务系统，多用于Oracle数据库服务器或Hadoop系统。应充分发挥资源池化优势，提升资源利用率，各业务系统优先使用虚拟化资源池。

2. 计算资源划分

城轨云平台通过使用主机虚拟化技术，形成计算资源池，结合城轨业务实际需求，建设x86服务器组成的虚拟化资源池和裸金属资源池。利用虚拟化提高资源利用率的同时，为数据库应用提供高CPU、高IO的裸金属服务器，满足业务系统对不同计算能力的需求。



虚拟资源池是将物理服务器进行虚拟化，如 CPU 虚拟化、内存虚拟化、设备 I/O 虚拟化等。实现在单一物理服务器上运行多个虚拟服务器（虚拟机），不同虚拟机之间相互隔离、互不影响，可运行不同操作系统，提供不同应用服务。虚拟机是云平台提供计算资源的主要类型。

OpenStack 体系结构中，通过预先配置好 PXE、IPMI 等服务，完成裸金属的相关配置之后，使用 Nova API 来实现一个物理机实例的创建及生命周期的管理。因此，云平台通过执行一系列操作完成一台或多台物理服务器的快速交付，而不会对其进行虚拟化，用户可以如传统架构中一样使用裸金属服务器。对于 Oracle 数据库、数据挖掘等可使用裸金属服务器。

3. 有效可分配计算资源

● 单物理服务器-可分配 vCPU 计算

每台虚拟化高性能服务器承载 vCPU 数量计算方法如下：

$\text{vCPU 数量} = (\text{CPU 颗数} \times \text{每颗 CPU 物理核数量} \times 2 - \text{虚拟化层占用逻辑核数量}) \times \text{服务器虚拟机资源预留}$ ；

在进行 vCPU 资源分配时需考虑以下几个因素：

- 资源分配仅考虑静态分配，业务系统虚拟机运行场景虚拟化复用比按 1 考虑；
- 服务器虚拟化层占用逻辑核占用率：按不超过 10% 考虑；
- 服务器虚拟机预留资源：用于虚拟机迁移、业务系统临时扩容等，按不超过 30% 考虑；

因此，对于 4 路 16 核、开启 HT 多线程的服务器而言，单台设备 vCPU 可分配数为：

$$\text{vCPU 数量} = (4 \times 16 \times 2 - 4 \times 16 \times 2 \times 10\%) \times 70\% = 4 \times 16 \times 2 \times 63\% \approx 80;$$

通过收集各业务系统 vCPU 需求总量，可计算出实际需要的最小物理 CPU 数量，进而可得出所需虚拟化服务器数量。在不考虑临时扩容的情况下，系统保留了 30% 的冗余性。

● 单物理服务器-可分配内存计算

每台虚拟化高性能服务器可分配内存计算方法如下：

可分配内存=（物理内存总量 - 虚拟化层占用）×服务器虚拟机资源的最佳占用率；

在进行内存资源划分时需考虑以下几个因素：

a. 服务器虚拟化层占用逻辑核占用率：按不超过 10%考虑；

b. 服务器虚拟机预留资源：用于虚拟机迁移、业务系统临时扩容等，按不超过 30%考虑；

因此，对于物理内存为 512G 的服务器，单台设备可分配的内存为：

可分配内存=（512 - 512×10%）×70% =512×63%≈322G；通过收集各业务系统内存需求总量，通过可分配内存计算方法以及 CPU 计算得出的机器数量。

4. 动态资源利用率估算

上一节的计算结果是指可分配资源，即有多少资源可被分配给业务系统。即使所有的可分配资源都分配完之后，当系统运行起来还会存在一个动态资源利用率。这个动态资源利用率需要实际测量，可用于衡量物理主机真实的负载。

计算公式：

真实负载 = 虚拟化占用比 + 可用资源占比*分配率*利用率

下表估算了在不同场景下，一台物理服务器的真实负载情况。其中紧急状态是指因为其它服务器故障，部分业务系统迁移至本机，达到 90%的分配率的场景。

	完全分配（70%分配率）	紧急状态（90%分配率）
业务系统平均资源利用率 30%	28.9% $0.1+0.9*0.7*0.3$	34.3% $0.1+0.9*0.9*0.3$
业务系统平均资源利用率 60%	47.8% $0.1+0.9*0.7*0.6$	58.6% $0.1+0.9*0.9*0.6$

经估算，只有当业务系统平均利用率>30%以上，才能有效使用硬件资源。但如果超过 60%，可能会出现因为负载过高而带来整体性能下降的风险。建议后续系统资源优化同样可以遵循利用率>30%而<60%的策略。

3.3.2. 存储资源

1. 设计原则

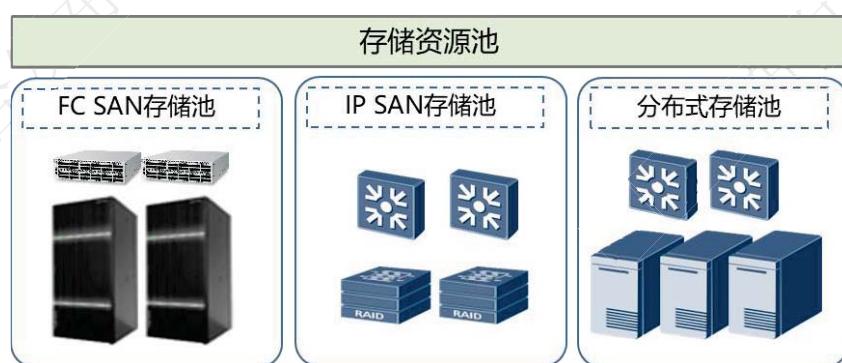
存储是城轨云平台的基础，各业务数据、虚拟机文件、配置数据等均保存在存储系统，因此，要求存储资源设计具备以下特点：

- 先进性原则：存储技术构成先进，符合技术发展趋势，能够适应在不同 IT 架构下进行大规模数据存储的需要。

- 稳定性原则：存储系统应 7x24 小时稳定运行，并能保证重启系统的稳定性。提供成熟可靠的运行管理、监控、故障处理等技术手段。
- 经济性原则：按照业务类型提供差异化服务等级，通过支持不同级别的存储，满足存储需求的同时，有较好的性能价格比。

2. 存储划分

存储资源池在性能（IOPS、带宽等）及可用性（存储设备类型、磁盘 RAID 级别、存储级容灾能力等）不同，可分为不同的存储资源池满足业务系统对不同性能、容量、可靠性要求。同时配置一定比例的固态硬盘（SSD）实现分级存储，满足业务系统对更高 I/O 能力需求。按照不同实现可将存储分为：FC SAN 存储、IP SAN 存储、分布式存储、主机存储等。



● FC SAN 存储池

采用光纤通道连接交换机、存储阵列和服务器主机，建立专用于数据存储的区域网络。FC SAN 存储被广泛验证并应用于关键业务系统，提供高性能及高可靠性存储资源，建议用于生产业务系统。

● IP SAN 存储池

采用以太网通道连接交换机、存储阵列和服务器主机，组建数据网络。IP SAN 在发挥 SAN 存储的稳定性、性能的同时，能有效降低成本，可用于各业务系统的云桌面系统或非关键业务。

● 分布式存储池

将通用的 x86 存储服务器上的本地磁盘进行整合、池化，建立大规模的分布式存储资源池，提供标准的块存储数据访问、文件系统、对象存储访问接口，相比 SAN 存储，成本明显降低，适用于 CCTV 系统视频存储、图片、流媒体等。通常是存储容量超过 PB 规模，且对数据读写性能要求不高的场景使用分布式存储。

● 主机存储

主机存储是指服务器上的本机磁盘。在 Hadoop 大数据架构中，就是使用本机磁盘，在多台主机上实现集群的存储和计算功能。在 Hadoop 集群中，不需要配置额外的存储系统，但主机的磁盘配置要满足需求。

在规划 SAN 存储池容量时，额外还需要考虑 2 点：

- SSD 和 HDD 容量：SSD 速度快价格高，一般用于系统的系统盘，HDD 容量大，一般用于系统的数据盘。这两部分容量需分别统计和计算。
- 冗余预留量：需为 SAN 存储资源留出一定预留量。存储资源与计算资源不同，计算资源包含静态分配和动态使用 2 部分，后期有根据实际使用情况调整的空间。存储资源在分配完成之后，如果想缩减容量，操作会非常繁琐，甚至可能影响业务系统运行。存储资源的这种特性，需要存储池有一定预留。

3. 容量计算

计算 SAN（FC SAN & IP SAN）存储池容量：

- 虚拟机系统盘容量=虚拟机本身的系统所需空间+虚拟机内存规格，建议使用 SSD 盘，且容量不小于 100G
- 虚拟机数据盘容量=虚拟机本地数据所需空间
- 存储冗余率建议不低于 30%，备份快照预留建议不低于 SSD 容量的 50%
- 建议 SAN 存储池 SSD 存储总量 = 100G * 虚拟机系统数量 * 1.5
- 建议 SAN 存储池 HDD 存储总量 = 各业务系统数据需求总容量 * 1.3

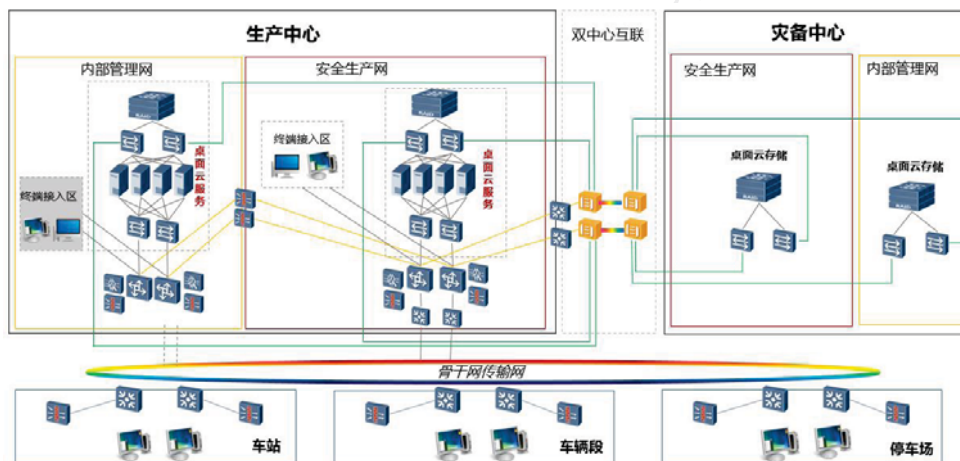
计算分布式存储池/主机存储池容量：

- 用于存储大量数据的存储系统，数据是逐步积累的，不会像 SAN 系统那样初期就会分配完。所以只需考虑业务需求即可，无需考虑容量冗余
- 容量建议仅考虑以当前需求为准，建议考虑存储 3 年数据
- 这类存储系统的特点是能够平滑扩容，如果后续出现新需求，可通过扩容方式满足。

3.4. 桌面云设计

3.4.1. 硬件部署架构

城轨云在主用中心的安全生产网、内部管理网分别部署云桌面服务器及云桌面存储资源，分别为安全生产网、内部管理网内的业务提供桌面云服务。同时在灾备中心的安全生产网、内部管理网分别部署云桌面存储资源，用于主用中心的桌面云数据同步到灾备中心。



对于桌面云的管理终端，建议采用 PC 机，正常情况下，主用中心安全生产网的桌面云管理终端从终端接入分区接入到安全生产网内，对桌面云进行管理；安全生产网和企业内部管理网桌面云系统可以设置统一的管理终端，也可以设置独立的管理终端，如果安全生产网和企业内部管理网独立设置桌面云的管理终端，主用中心的内部管理网的桌面云的管理终端从终端接入分区接入到内部管理网内，对桌面云进行管理。

主用中心内部管理网部署内部管理桌面云的计算、存储、网络资源，提供完整的桌面云服务，同时在灾备中心内部管理网部署一套桌面云存储，作为主用中心桌面云业务的数据异地存储资源，主用中心的桌面云数据实时同步到灾备中心的存储。

3.4.2. 桌面云计算资源规划

桌面云系统以服务器虚拟化为基础，允许多个用户桌面以虚拟机的形式独立运行，同时共享 CPU、内存、网络连接和存储器等底层物理硬件资源。

相比起业务系统，桌面云的使用相对宽松，往往不需要那么多高密度的 CPU 计算工作，在 CPU 复用比设置上要比业务系统更加宽松，可以大于 1。复用比可根据不同网域设置不同数值，在呼和浩特城轨云实际部署中，安全生产网云桌面系统的 CPU 复用比为 1.5，内部管理网云桌面系统的 CPU 复用比为 2。

桌面云需要有后台管理系统，呼和浩特项目上每套云桌面系统需要 40 vCPU 和 80G 内存，这部分资源可以和云桌面业务系统所需资源相加，作为总体资源需求。

单台云桌面物理服务器等效 vCPU 数量的计算：

$$\text{vCPU 数量} = (\text{CPU 数量} \times \text{每颗 CPU 物理核数量} \times 2 - \text{虚拟化层占用}) \times \text{服务器虚拟机资源占用率} \times \text{虚拟化复用比};$$

- 服务器虚拟化层占用逻辑核占用率：按不超过 10%考虑；
- 服务器虚拟机预留资源：用于虚拟机迁移、业务系统临时扩容等，按不超过 30%考虑；

以呼和浩特云平台实际部署配置为例，

安全生产网：vCPU = $(4*16*2 - 4*16*2*10\%)*70\%*1.5 = 121$

内部管理网：vCPU = $(4*16*2 - 4*16*2*10\%)*70\%*2 = 161$

单台云桌面物理服务器的内存资源的计算：

可分配内存 = (物理内存总量 - 虚拟化层占用) × 服务器虚机资源占用率；

在进行内存资源划分时需考虑以下几个因素：

- a. 服务器虚拟化层占用逻辑核占用率：按不超过 10%考虑；
- b. 服务器虚机预留资源：用于虚机迁移、业务系统临时扩容等，按不超过 30%考虑；

呼和浩特桌面云使用的是物理内存为 512G 的服务器，单台设备可分配的内存为：

可分配内存 = $(512 - 512 \times 10\%) \times 70\% = 512 \times 63\% \approx 322\text{G}$ ；

因为在云桌面系统计算资源有超分，在分配计算资源的时候需要注意内存/CPU 比，保证资源分配的均衡性。如在内部管理网，尽量保持内存：CPU 不大于 2，如 2 vCPU / 4G 内存、4 vCPU / 8G 内存。

3.4.3. 桌面云存储资源规划

存储资源主要为虚拟桌面提供系统空间、数据空间，以及桌面云管理系统所需要的空间。

桌面云系统的存储资源可采用传统 SAN 的形式，或采用超融合形式。呼和浩特城轨云采用的是 IP SAN 存储阵列，桌面云存储阵列双上行至 IP 交换机，交换机与存储控制器互联，存储控制器根据桌面云数量，可灵活配置硬盘框数量。安全生产网的桌面云业务在主用中心、灾备中心分别部署一套 IP SAN 存储，为安全生产桌面云服务提供云桌面数据存储服务；内部管理网业务在主用中心、灾备中心分别部署一套 IP SAN 存储，为内部管理桌面云服务提供云桌面数据存储服务。

桌面云对存储资源需求：

虚拟机系统盘容量 = 虚拟机本身的系统所需空间 + 虚拟机内存规格，建议使用 SSD 盘，且容量不小于 100G

虚拟机数据盘容量 = 虚拟机本地数据所需空间

共享存储总量 = (虚拟机系统盘容量 + 虚拟机数据盘容量) * (1 + 存储冗余率 + 备份快照预留)

存储冗余率建议不低于 20%，备份快照预留建议不低于 30%。

3.4.4. 桌面云网络规划

使用桌面云的用户可以通过瘦客户端、或者个人电脑接入并访问到后端的桌面云服务，瘦客户端的接入网络可以是百兆或千兆 GE 网口。瘦客户端所需带宽：普通办公约为 2~4Mbps，高清视频为 20Mbps。

呼和浩特城轨云的桌面云系统部署共两套，分别部署在主用中心的数据中心机房的安全生产网和内部管理网中，采用独立 VDC。桌面云分区设置两台独立的接入交换机，桌面云服务器双接入至两台接入交换机，由接入交换机与数据中心核心交换机对接。桌面云网络通信平面划分为业务网、存储网和管理网。三个网络之间是隔离的，保证最终用户不能破坏基础平台。

存储网络：存储网络通过多路径确保链路冗余，服务器与存储设备通过存储网络直接互通。存储设备为虚拟机提供存储资源，但不直接与虚拟机通信，而通过虚拟化平台转化，采用 IP SAN 存储，存储网络采用 IP 交换机。

业务网络：为用户提供业务通道，为虚拟机虚拟网卡的通信平面，对外提供业务应用。桌面云远程访问协议与虚拟机访问外部应用系统均经过此网络。业务网络可通过 SDN 控制器下发，实现网络灵活配置与隔离。

管理网络：负责整个桌面云系统的管理、业务部署、系统加载等流量的通信。

3.5. 灾备及备份

3.5.1. 容灾简介

容灾系统是指在相隔较远的异地，建立两套或多套功能相同的 IT 系统，互相之间可以进行健康状态监视和功能切换，当一处系统因意外（如火灾、地震、意外停电等）停止工作时，整个应用系统可以切换到另一处，使得该系统功能可以继续正常工作。容灾技术是系统的高可用性技术的一个组成部分，容灾系统更加强调处理外界环境对系统的影响，特别是灾难性事件对整个 IT 节点的影响，提供节点级别的系统恢复功能。

3.5.1.1. 容灾衡量指标及等级

衡量容灾系统的主要指标有 RPO（Recovery Point Object，灾难发生时允许丢失的数据量）、RTO（Recovery Time Objective，系统恢复的时间）。

RPO 是指业务系统所允许的灾难过程中的最大数据丢失量（以时间来度量），这是一个与灾备系统所选用的数据复制技术有密切关系的指标，用以衡量灾备方案的数据冗余备份能力。

RTO 是指“将信息系统从灾难造成的故障或瘫痪状态恢复到可正常运行状态,并将其支持的业务功能从灾难造成的不正常状态恢复到可接受状态”所需时间,其中包括备份数据恢复到可用状态所需时间、应用系统切换时间、以及备用网络切换时间等,该指标用以衡量容灾方案的业务恢复能力。例如,灾难发生后半天内便需要恢复,则 RTO 值就是十二小时。

显然,具有零 RTO、零 RPO 的灾难恢复方案是用户最期望的,但受系统性能要求、适用技术及成本等方面的约束,此方案是不契合实际的。所以,用户在选择容灾方案时应该综合考虑灾难的发生概率、灾难对数据的破坏力、数据所支撑业务的重要性、适用的技术措施及自身所能承受的成本等多种因素,理性地作出选择。

参考“信息系统灾难恢复规范”国家标准 GB/T 20988-2007 的规范,以及不同容灾能力等级,与 RPO\RTO 对应关系如下:

容灾等级	简介	RPO	RTO
第1级	备份基本支持	1天至7天	2天以上
第2级	备用场地支持	1天至7天	24小时以上
第3级	电子传输和部分设备支持	数小时至1天	12小时以上
第4级	电子传输及完整设备支持	数小时至1天	数小时至2天
第5级	实时数据传输及完整设备支持	0至30分钟	数分钟至2天
第6级	数据零丢失和远程集群支持	0	数分钟

3.5.1.2.容灾建设模式

1. 同城容灾

同城容灾是在同城或相近区域内 ($\leq 200\text{KM}$) 建立两个数据中心:一个为数据中心,负责日常生产运行;另一个为灾难备份中心,负责在灾难发生后的应用系统运行。同城灾难备份的数据中心与灾难备份中心的距离比较近,通信线路质量较好,比较容易实现数据的同步复制,保证高度的数据完整性和数据零丢失。同城灾难备份一般用于防范火灾、建筑物破坏、供电故障、计算机系统及人为破坏引起的灾难。

2. 异地容灾

异地容灾主备中心之间的距离较远 ($> 200\text{KM}$), 因此一般采用异步镜像,会有少量的数据丢失。异地灾难备份不仅可以防范火灾、建筑物破坏等可能遇到的风险隐患,还能够防范战争、地震、水灾等风险。由于同城灾难备份和异地灾难备份各有所长,为达到最理想的防灾效果,数据中心应考虑采用同城和异地各建立一个灾难备份中心的方式解决。

3. 两地三中心

结合近年国内出现的大范围自然灾害,以同城双中心加异地灾备中心的“两地三中心”的灾备模式也随之出现,这一方案兼具高可用性和灾难备份的能力。

同城双中心是指在同城或邻近城市建立两个可独立承担关键系统运行的数据中心，双中心具备基本等同的业务处理能力并通过高速链路实时同步数据。日常情况下可同时分担业务及管理系统的运行，并可切换运行；灾难情况下可在基本不丢失数据的情况下进行灾备应急切换，保持业务连续运行。

异地灾备中心是指在异地的城市建立一个备份的灾备中心，用于双中心的数据备份，当双中心出现自然灾害等原因而发生故障时，异地灾备中心可以用备份数据进行业务的恢复。

3.5.2. 容灾关键技术

3.5.2.1. 数据同步技术

在构建容灾系统所涉及的诸多要素中，数据复制技术是基础，只有保证了数据的安全可用，应用或业务的恢复才有可能。正常情况下系统的各种应用在数据中心运行，数据存放在数据中心和灾难备份中心两地保存。当灾难发生时，使用备份数据对工作系统进行恢复或将应用切换到备份中心。

数据复制技术的选择决定灾备系统的 RPO 指标，灾难备份系统中数据备份技术的选择应符合数据恢复时间或系统切换时间满足业务连续性的要求。

根据不同容灾方案所采用数据复制技术位于 IT 架构不同层面，数据复制可分为基于存储层的复制、基于主机层复制和基于数据库的复制。

1. 基于存储层的远程复制

基于存储底层的复制技术核心是利用存储阵列自身对数据块的复制技术实现数据从主用中心的远程拷贝，从而实现对主用中心数据的灾难性保护。主用中心发生灾难时，可以利用灾备中心的数据建立运营支撑环境，为继续运营提供 IT 支持。

通过存储底层复制技术实现数据同步，有两种实现模式：同步工作模式与异步工作模式。

- 同步工作模式

同步工作模式是服务器向存储写数据后（写入 cache），每一个 IO 会同时写往远程灾备中心的存储阵列，并且在确认往本地和远程都写成功后才会应答服务器，表示写操作成功。

同步工作模式会保证主备中心的存储阵列中的应用数据完全一致，当主用中心发生灾难时，灾备中心的数据完全保留了主用中心灾难发生前的数据，可以实现 RPO 为零，适用于对业务数据安全性要求较高的业务系统。由于主用中心需要等待灾备中心写完后返回确认信息，对应用处理性能有一定的影响，为避免对生产系统性能的影响，同步方式通常在近距离范围内（FC 连接通常是 200KM 范围内，实际部署多在 35KM 之内）。

- 异步工作模式

异步工作模式是服务器向存储写数据后（写入 cache），主用中心存储立即返回给服务器“写完成”，服务器可以继续写 IO 操作。同时，主用中心存储阵列利用自身机制将写 IO 写入灾备中心存储阵列，实现数据保护。

采用异步方式服务器不需要等待灾备中心存储完成写操作，因此对应用处理性能影响较小，适用于双中心距离较远的情况，但是存在数据丢失的风险，通常在远距离通信链路带宽有限的条件下实施。

对于基于存储层完成的数据同步，不论是同步方式还是异步方式，通常必须采用同一厂商同系列的存储阵列，但是基于存储层完成的数据同步，由于在最底层，对主机、应用环境等相关技术影响最小，非常适合主机和业务系统很多、环境很复杂的情况。

云平台通过对存储远程复制中各环节进行封装，将复杂的底层操作封装为用户可申请的服务，如华为云平台的 CSDR（Cloud Server Disaster Recovery 云服务器容灾）服务。用户可通过在运营界面申请容灾服务，将需要保护的虚拟机创建为容灾实例，云平台调用相关接口实现主备双中心存储远程复制及双中心主机映射。当主用中心发生灾难时，可在灾备中心云管理平台中将容灾保护的实例恢复，业务系统可在此基础上恢复应用及业务，同步复制模式下可实现 $RPO \approx 0$ ，RTO 小时级容灾能力。

2. 基于存储同步的双活存储

当业务系统要求当灾难发生时，系统能继续提供服务时，往往需要搭建双活数据中心，当一个数据中心发生设备故障时，业务自动切换到另一个数据中心，解决了存储远程复制容灾方式中业务无法自动切换的问题。双活数据中心的建设基础便是双活存储。

通过数据双写和 DCL（Data Change Log）机制实现存储层数据的双活，两个数据中心同时对主机提供数据读写能力。在业务运行中，数据变更可通过双写和 DCL 来完成同步。双写可以使得应用服务器的 I/O 请求同时下发到本端 Cache 和远端 Cache，从而保证本端 Cache 与远端 Cache 的变更数据一致性。在一个数据中心故障时，DCL 可以记录业务运行中数据中心的变更数据。待故障恢复后，同时跟踪变更数据同步到该数据中心的存储设备中，以防止变更的数据在同步过程中出现遗漏。

呼和浩特城轨云的云硬盘高可用（VHA）的数据同步（主要是指云主机存储），就是基于双活存储的具体应用。

3. 基于数据库的复制

基于数据库的复制技术大致分为两类：数据库软件自身提供的数据库容灾功能和第三方提供的数据库复制。

以 Oracle 数据库方案举例，Active Data Guard 是从 Oracle 11g 开始支持的方案。通过 Active Data Guard，数据中心的主用 Oracle 数据库数据实时同步复制到另一个数据中心的备用 Oracle 数据库，在主用 Oracle 数据库可读写的同时，备用 Oracle 数据库也支持只读功能，

从而可提供实时报表、数据备份等业务。并且，备用 Oracle 数据库支持数据块健康扫描功能，主用 Oracle 数据库数据块损坏后可通过备用 Oracle 数据库数据进行反向恢复。

通过 Active Data Guard 技术将同城主用数据中心的主数据库数据实时同步复制到同城灾备数据中心备用数据库，两边的灾备业务只访问主用 Oracle 数据库，对同城灾备数据中心的业务来说存在次优路由的情况，由于同城灾备数据中心之间通过 DWDM 波分互联，可以支撑跨中心访问数据库业务的正常运行。

3.5.2.2.应用切换技术

容灾业务系统通过数据同步以及应用倒切后，可实现应用系统恢复，但如果需要继续对外提供业务则需要应用切换。目前，主要采用的应用切换技术包括：DNS 切换、负载均衡设备、修改连接配置文件。

DNS 切换：访问应用时，通常会直接使用主机的 IP 地址进行访问，在这种情况下如果发生了容灾切换，原访问 IP 将不可达，造成业务中断。当采用 DNS 域名切换技术时，所有的应用通过域名来访问，而不是直接使用主机的 IP 地址。对于外部业务，可通过向运营商申请相应的 DNS 服务器，对主用中心、灾备中心各申请相应的 DNS 服务，通过运营商 DNS 切换机制实现对外服务的切换。对于内部业务，主用中心和灾备中心各部署一台 DNS 服务器，负载主机的域名解析。主用中心为主 DNS，灾备中心为备份 DNS，两台 DNS 服务器内容自动保持完全同步，对于每个应用服务器的域名，DNS 服务器都保持两个 IP 地址，主 IP 指向主用中心，备份 IP 指向灾备中心。客户端设置两个 DNS 服务器，当主用中心主服务器出现故障，主 DNS 服务器无法连接到主服务器时，会自动将 DNS 解析为灾备中心服务器 IP，从而实现单个应用的自动切换。

基于负载均衡切换：通过在应用服务器集群前部署负载均衡设备，根据已配置的均衡策略将请求在服务器集群中分发，并可以采取静态设置或动态调配的方式。负载均衡能够针对各种应用服务状态进行检测，收集相应信息作为选路依据，包括 ICMP、TCP、HTTP、FTP、DNS 等。通过对应用状态的识别，使得业务可以在主用中心和灾备中心之间进行切换。

修改连接配置文件：通过修改客户端主机中的连接配置文件，将连接目标地址由主用中心修改为灾备中心，同样可以实现双中心间访问切换，此方式存在较长的切换时间。

3.5.3. 城轨云业务容灾

3.5.3.1.需求分析

城市轨道交通作为城市公共交通的重要组成部分，在承担大规模客运服务的同时，需要保障行车安全以及良好的乘客体验。因此，要求行车控制系统及其配套系统具备一定的可靠性保障，同时要求承载系统运行平台具备容灾能力。

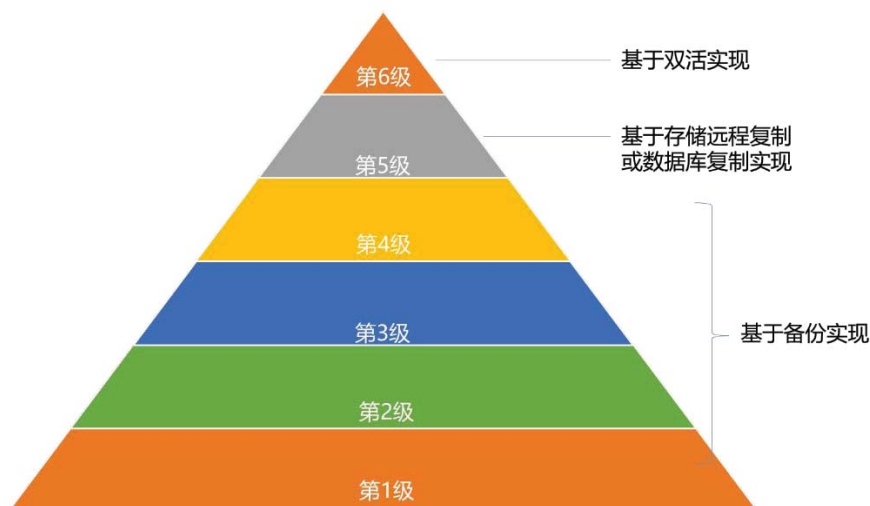
城市轨道交通作为公共交通，其服务对象为当前城市出行乘客，城轨业务访问范围相对集中。对于城轨业务的容灾方案重点考虑：1、单个系统出现对应用故障，将会导致生产业务中断；2、多业务系统故障，将会导致业务中断；3、个别与行车直接相关的关键业务出现故障时可继续提供关键业务；4、业务系统故障时对数据的保护。暂不考虑对于发生大范围的自然灾害时业务连续性，因此，对于城轨业务而言，同城主备数据中心架构可满足大多数业务灾备需求。城轨云平台除提供承载正常业务的主用中心外，还提供线网级灾备中心云平台，在灾备中心统一部署轨道交通领域运营生产系统、企业管理信息系统、乘客服务管理系统所需的计算、存储、网络资源。

对于业务系统而言，根据其自身业务属性以及对数据丢失容忍度进行容灾分析：

- 1) 列车自动监控系统（ATS），作为信号系统的大脑，通过对列车运行监控、自动排列进路、自动列车调整、自动生成时刻表、自动记录和统计运行数据并生成报表、自动检测设备运行状态等实现对列车运行的监督和控制，辅助调度员对全线列车进行管理。ATS 系统的运行状态将对运营生产具有直接影响关系，因此，在发生意外灾害或系统故障时，要求 ATS 系统有足够的保护机制。对于线网及运营环境，ATS 除降级至车站控制外还要求具有中心级容灾能力，当主用中心发生故障时，可以使用灾备中心 ATS，继续对全线列车进行自动监控。
- 2) 综合监控系统（ISCS），在地铁运营中起着重要作用，有些地铁公司采用深度集成方案，把供电、环境监控、火灾报警等系统集成到一个系统中，通过标准接口将各子系统和综合监控系统相连，实现全过程、全方位监控。在高度集成的情况下，需要保证系统具备容灾能力，当发生灾难时，可在灾备中心继续对运营环境进行监控。
- 3) 自动售检票系统（AFC），作为与乘客相关的业务系统，在故障发生时仍然能保证乘客顺利进出站以及票款及时扣除。同时，当前互联网支付日益普及，手机支付已成为重要环节。对于 AFC 系统而言，除降级为站控模式处理紧急情况外，需要增加线网级应用系统的容灾能力。当主用中心故障时，可保证交易数据不丢失，同时灾备中心可继续提供关键业务能力。
- 4) 专用通信系统，作为运营生产的重要子系统，当主用中心故障发生时，要确保数据不丢失。

3.5.3.2.容灾方案

通过对容灾等级和关键容灾技术分析，在城轨业务中大致可将容灾实现划分为三类：基于备份实现、基于存储远程复制或数据库复制实现、基于双活实现。

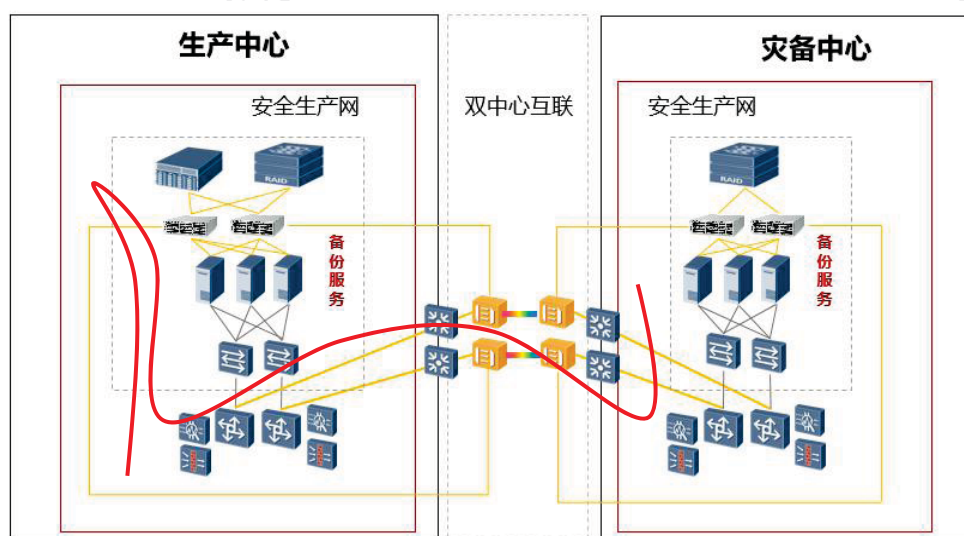


1. 基于备份实现

主用中心和灾备中心分别建设备份系统，在主用中心设置备份系统，满足容灾等级为4级以下业务，如PIS、PBE、CAS等业务的本地备份需求。通过备份软件将数据（操作系统、数据库、文件或虚拟机等）在主用中心本地进行周期性数据备份，如每周进行一次全量备份，每日进行一次增量备份，备份执行时间选择夜间停运后低峰期完成。同时，备份系统也可以作为其它容灾方案的补充，同时为高容灾等级的业务提供数据保护。

灾备中心设置异地备份系统，满足安全生产网业务系统的异地备份需求，主用中心的业务系统数据在完成本地的数据备份后，由本地备份系统通过远程数据复制的方式将本地备份完成的数据传送同步至灾备中心的备份系统进行远端的异地数据备份。

主用中心和灾备中心的备份链路建议采用10GE通道进行互联，主用中心本地备份数据通过双中心互联的备份链路传输同步到灾备中心的备份系统中，完成异地备份的功能。



2. 基于存储远程复制或数据库复制实现

综合监控 ISCS、门禁系统 ACS、自动售检票系统 AFC 等业务系统中部分重要数据不允许发生丢失，利用备份系统保护的基础上，可增加基于存储远程复制或数据库复制实现的容灾保护。

利用主用中心与灾备中心存储的远程复制功能，将主用中心需要保护的数据采用同步复制或异步复制的方式保护至灾备中心，灾备中心配置一定的计算能力用于恢复灾备数据。对于 OpenStack 环境配置存储远程复制时需要灾备中心存在计算资源且存储的复制及切换由云平台实现，云平台将其封装为容灾服务，无需手工操作底层存储配置。当主用中心发生故障时，可通过手工或自动的方式在云管理平台进行切换，业务系统可在灾备中心恢复受保护的应用系统。由于存储远程复制存在切换时间，因此，基于此方式实现的容灾方案 RTO>0，故障发生时存在业务中断现象。

对于业务系统仅需要保护数据库数据不丢失时，除使用云平台提供的容灾服务外，也可采用主备数据中心各自部署数据库，利用数据库软件容灾功能实现对数据的保护。

3. 基于应用双活实现

ATS、AFC 互联网售票子系统由于其业务的特殊性，在主用中心故障发生时，需要提供连续的业务能力，保障列车运行安全以及乘客刷二维码正常进出站。因此，对于 ATS 和 AFC 互联网售票子系统而言，在保障数据容灾的基础上提供业务连续能力。

通过数据中心互连技术实现数据中心的网络通道建设，同城数据中心采用 DWDM 波分设备互联的方案，实现高宽带低时延传输，满足数据传输需求。前端网络灾备建设使用 GSLB（全局负载均衡）技术将业务访问分发到主用生产数据中心。灾备应用跨数据中心部署，用户访问到其中任何一个数据中心的申请均可以获取到相同的业务服务，从而实现应用在灾备数据中心同时对外提供服务。数据库采用集群技术保证两边的数据库数据的一致性；存储采用双活技术保障数据一致性。

基于应用双活实现的容灾机制对业务系统应用自身有强依赖关系，需要底层存储、数据库到应用系统均实现双活，同时配合适当的应用切换技术，才能实现故障发生时提供连续业务能力。

呼和浩特城轨云提供了应用双活的能力，但 ATS 系统在迁移至云平台前已有成熟的业务容灾方案，其容灾方式由应用系统自身实现。在后续城轨云建设过程中，可由业务系统先提出灾备对平台的需求，再由云平台规划总体容灾的方案。

3.6. 网络安全

《中华人民共和国网络安全法》第 31 条规定“对于国家关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护”。城轨云平台作为城市轨道交通的基础设施平台，必须对整个平台进行安全保护，并达到要求的安全等级保护级别。协会颁布的《智慧城市轨道

交通 信息技术架构及网络安全规范 第3部分：网络安全》中，对城轨云平台的安全有了系统的描述。明确要求安全生产网中部署的系统达到等保3级，内部管理网的系统达到等保2级。

2019年5月，国家颁布了新的《信息安全技术网络安全等级保护基本要求》2.0版本(以下简称“等保2.0”)。新的等保要求在多个领域所有加强。后续城轨云建设同样要求按照等保2.0标准进行评测。

3.6.1. 等保2.0标准

等保2.0相比《信息安全技术信息系统安全等级保护基本要求》(以下简称“等保1.0”)而言，增加了4个扩展要求：云计算安全扩展要求、移动互联安全扩展要求、物联网安全扩展要求和工业控制系统安全扩展要求。其中云计算安全扩展要求包含虚拟机，虚拟网络设备，虚拟安全设备的安全要求。

等保标准包含安全技术和安全管理两部分，相比等保1.0标准，等保2.0将技术要求分为以下5部分：

- 1) 安全物理环境：即等保1.0标准中的物理安全部分，包括机房的各类基础设施，如门禁、监控、火灾、双路供电和UPS等内容。
- 2) 安全通信环境：是等保1.0标准中网络安全部分的扩展，包括网络冗余架构设计、隔离、远程接入加密等内容。
- 3) 安全区域边界：是等保1.0标准中网络安全部分的扩展，包括和其它系统边界防护、访问控制、入侵防范、恶意代码防范等内容。需依照协会网络安全规范中对接口的要求进行防护，后有详述。
- 4) 安全计算环境：是等保1.0标准中主机安全、应用安全、数据安全及备份恢复3部分的合集及扩展。需对身份鉴别、访问控制、安全审计、可信验证、入侵防范、恶意代码防范、数据完整性、数据保密性、数据备份恢复和个人信息保护等方面进行测评。评测对象包括操作系统(包括宿主机和虚拟机操作系统)、网络设备(包括虚拟网络设备)、安全设备(包括虚拟安全设备)、移动终端数据库管理系统、中间件和系统管理软件及系统设计文档等内容。
- 5) 安全管理中心：为等保2.0新增部分，需提供集中的系统安全管理、综合安全审计、数据库审计、综合网管等功能。

城轨云平台安全防护在技术要求上主要关注安全物理环境，安全通信环境，安全区域边界和安全管理中心这四部分。针对安全计算环境的要求，建议云平台和业务系统的安全责任边界划分在虚拟机(裸金属服务器)之上，操作系统之下。从操作系统往上的安全工作由各业务系统自行负责。可根据实际项目要求，城轨云平台承担某些公共安全服务，如数据库审计、主机防病毒、漏洞扫描等。

《规范》中安全生产网要求等保三级而内部管理网要求等保二级，二级和三级技术要求的差异见下表。因为都是在一个基础设施平台之上，内部管理网等保二级中所有冗余要求（如供电冗余，链路及设备冗余，网络处理能力）都可由底层满足。其它安全要求可根据项目实际要求进行增强。

● 等保二级三级技术要求差异

等保要求	主要差异
安全物理环境	三级新增冗余供电要求
安全通信网络	三级新增链路和设备冗余要求
	三级新增网络的业务处理能力满足业务高峰期需要
	三级新增数据传输保密性要求
安全区域边界	三级增加基于应用协议和应用内容的访问控制要求
	三级增加在关键节点的未知威胁检测要求
	三级新增基于重要业务带宽保障
	三级新增垃圾邮件防护要求
安全计算环境	三级新增主机入侵检测要求
	三级新增异地容灾要求

● 等保二级关键安全要求：

等保技术要求	子项	主要内容
安全通信网络	网络架构	分区隔离

	通信传输	采用校验技术保证通信过程中数据的完整性
	可信验证	基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并将验证结果形成审计记录送至安全管理中心
安全区域边界	边界防护	跨越边界的访问和数据流通过边界设备提供的受控接口进行通信
	访问控制	基于五元组的会话状态进行访问控制、策略优化
	入侵防范	在关键网络节点处监视网络攻击行为
	恶意代码防范	恶意代码检测和清除，防护机制支持升级和更新
	安全审计	网络行为审计
安全计算环境	身份鉴别	身份唯一性、鉴别信息复杂度定期更换、登录失败处理功能、远程管理过程中防鉴别信息被窃听
	访问控制	用户权限管理、管理用户权限最小化
	安全审计	用户行为审计
	入侵防范	检测入侵行为、非使用端口关闭、管理终端限制、发现已知漏洞
	恶意代码防范	安装防恶意代码软件，防护机制支持升级和更新
	数据完整性	数据防篡改

	数据备份恢复	数据本地备份和恢复、批量数据异地备份
	剩余信息保护	鉴别信息、敏感信息缓存清除
	个人信息保护	个人信息最小采集原则、访问控制
安全管理中心	系统管理	应对系统管理员进行身份鉴别、应通过系统管理员对系统的资源和运行进行配置、控制和管理
	审计管理	应对安全审计员进行身份鉴别、应通过安全审计员对审计记录应进行分析，并根据分析结果进行处理

● 等保三级关键安全要求：

等保技术要求	子项	主要内容
安全通信网络	网络架构	分区隔离
	通信传输	采用校验技术保证通信过程中数据的完整性
	可信验证	基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并将验证结果形成审计记录送至安全管理中心
安全区域边界	边界防护	跨越边界的访问和数据流通过边界设备提供的受控接口进行通信

	访问控制	五元组过滤、内容过滤、策略优化、基于应用协议和应用内容的访问控制
	入侵防范	已知威胁防护、新型网络攻击行为的分析、记录攻击源 IP&类型&时间并遭受攻击时告警
	恶意代码防范	网络防病毒、垃圾邮件过滤
	安全审计	网络行为审计、用户行为单独审计和数据分析
安全计算环境	身份鉴别	身份唯一性、鉴别信息复杂度，口令、密码技术、生物技术等双因子及以上认证且其中一种必须为密码技术
	访问控制	用户权限管理、管理用户权限最小化
	安全审计	用户行为审计
	入侵防范	检测入侵行为、非使用端口关闭、管理终端限制、发现已知漏洞
	恶意代码防范	安装防恶意代码软件，防护机制支持升级和更新、可信验证
	数据完整性	数据防篡改
	数据备份恢复	数据本地备份和恢复、提供异地实时备份功能、数据处理系统热冗余
	剩余信息保护	鉴别信息、敏感信息缓存清除

	个人信息保护	个人信息最小采集原则、访问控制
安全管理中心	系统管理	应对系统管理员进行身份鉴别、应通过系统管理员对系统的资源 and 运行进行配置、控制和管理
	审计管理	应对安全审计员进行身份鉴别、应通过安全审计员对审计记录应进行分析，并根据分析结果进行处理
	集中管控	特定管理分区、统一网管和检测、日志采集和集中分析、安全事件识别告警和分析、安全策略集中管理
	安全管理	应对安全管理员进行身份鉴别、应通过安全审计员对审计记录应进行分析，并根据分析结果进行处理

安全管理主要分成以下 5 个部分，具体细则需要和城轨云运维一起考虑：

1. 安全管理制度：建立日常管理活动中常用的安全管理制度
2. 安全管理机构
 - 1) 岗位设置：设置系统管理员，安全审计员及安全管理员等岗位，定义各工作岗位的职责。
 - 2) 人员配置：配置相应数量的各级管理员。
 - 3) 授权和审批：根据各部门和岗位职责明确授权审批事项，审批部门和批准人等。
3. 安全管理人员
 - 1) 人员录用：由专门的部门或人员负责给新员工授权。
 - 2) 人员离岗：及时终止离岗人员的所有访问权限，取回相应的身份证件，钥匙及机构提供的相关软硬件设备。
 - 3) 安全意识教育和培训：对各类人员进行安全意识教育和岗位技能培训，告知相关的安全责任和惩戒措施。
 - 4) 外部人员访问管理：保证外部人员访问受控区域前获得授权或审批。

4. 安全建设管理

- 1) 定级和备案：以书面形式向网安机构说明保护对象的安全保护等级及确定等级的方法和理由。
- 2) 安全方案设计：根据安全保护等级选择安全方案，依据风险分析结果补充和调整安全措施。
- 3) 产品采购和使用：采购和使用符合国家相关规定的安全产品。
- 4) 工程实施：指定或授权专门的部门或人员负责工程实施过程的管理。
- 5) 测试验收：工程或项目建设完成后应有安全性测试验收。
- 6) 系统交付：制定交付清单，根据交付清单对所交接的设备、软件和文档进行清点。对负责运维的技术人员进行相应的技能培训。
- 7) 服务供应商选择：供应商选择符合国家有关规定。需要与选定的供应商签订安全相关协议。

5. 安全运维管理

- 1) 环境管理：对机房的安全管理作出规定，包括物理访问、物品进出和环境安全等方面。指定专门的部门和人员负责机房安全，对机房出入进行管理。定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理。
- 2) 介质管理：将介质存放在安全的环境中，对各类介质进行控制和保护，实行存储环境专人管理，并根据存档介质额目录清单定期盘点。
- 3) 设备维护管理：对设备（含备份和冗余设备）、线路等指定专门的部门或人员定期进行维护管理。
- 4) 漏洞和风险管理：采取必要措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补。
- 5) 网络和系统安全管理：划分不同的管理员角色进行网络和系统的运维管理，明确各角色的责任和权限。指定专门的部门或人员进行账户管理，对申请账户、建立账户、删除账户等进行控制。
- 6) 恶意代码防范管理：对恶意代码防范要求做出规定，包括防恶意代码软件的授权使用、恶意代码库升级，恶意代码的定期查杀，对外来计算机或存储设备接入系统前进行恶意代码检查等。
- 7) 备份与恢复管理：规定备份信息的备份方式、备份频度、存储介质、保存期等。并识别需定期备份的重要业务信息、系统数据及软件系统等。
- 8) 安全事件处置：明确安全事件的报告和处置流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责。并及时向安全管理部门报告所发现的安全弱点和可疑

事件。

3.6.2. 安全管理设备

等保 2.0 的新增要求中，除了传统的主机及边界安全设备（如主机防病毒、防火墙、入侵检测、网闸、沙箱）之外，增加了很多对安全集中管理以及识别未知网络威胁的要求。建议城轨云的安全管理增加以下 4 类设备。

3.6.2.1. 运维审计堡垒机

运维审计堡垒机能够提供集统一管理能力，支持对主流厂商的路由器、交换机、防火墙、服务器等进行集中管理。监控与审计云平台所有运维人员的操作行为，全过程监控与记录运维人员对设备系统的操作行为，做到统一接入、统一认证、统一授权、统一审计，有效降低内部运维风险。

系统可根据需要划分多种角色，可设置用户多种状态。支持基于多种条件，灵活设置访问设备或系统的策略。支持 B/S、C/S 两种不同方式的运维接入，适应不同运维人员的运维习惯，两种运维方式能提供相同的操作方式和审计入口。

3.6.2.2. 日志审计

日志审计系统能提供多类型日志统一的采集、存储、审计功能，能够满足日志统一管理和分析、上网 NAT 追踪等多种应用场景。

日志审计系统能够根据日志特征对安全系统 Syslog 日志进行如下分类：攻击防范、流量监控、黑名单、地址绑定、操作命令、防火墙登录、策略命中、内容过滤等。日志审计还支持异步查询和细粒度查询，基础流量分析、应用流量分析、接口流量分析、对攻击或病毒等威胁事件的统计分析、用户威胁（网络安全分析）报表、网络安全分析、会话及 NAT 溯源分析、流量分析、上网行为分析，多维日志分析等功能。

日志审计系统能自动对每个用户的操作进行记录，并可由审计员进行审计。能自动对运行过程中的故障及重要状态变化进行记录，方便管理员了解系统运行情况。

3.6.2.3. 态势感知

态势感知系统能够从全网网络流量中提取关键信息，通过多维度风险评估，采用大数据分析关联单点异常行为，从而还原出 APT 攻击链，准确识别和防御 APT 攻击，避免核心信息资产损失。

态势感知系统支持采集第三方系统信息以及安全设备的 Syslog 日志，支持采集网络/安全设备上报的 Netflow 数据。能够支持网络协议识别、文件还原、异常触发抓包功能，支持流

量协议识别功能，支持应用协议的解析。能够根据发现的网络高级威胁生成联动策略，基于网络拓扑，决策安全策略与逻辑安全设备的匹配关系，将联动策略下发到网络安全设备。

3.6.2.4. 安全管理中心

依据等保规范 2.0 要求，安全管理中心应具有 3 种角色：系统管理员、审计管理员和安全管理员。这 3 个角色分别负责整个系统的管理工作。安全管理中心应具备如下能力：

系统管理：系统管理员只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计。系统管理员能够对系统的资源和运行进行配置、控制和管理，包括用户身份、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。

审计管理：只允许审计管理员通过特定的命令或操作界面进行安全审计操作。审计管理员能够对审计记录进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。

安全管理：只允许安全管理员通过特定的命令或操作界面进行安全管理操作，并对这些操作进行审计。安全管理员能对系统中的安全策略进行配置，包括安全参数的设置，主体、客体进行统一安全标记，对主体进行授权，配置可信验证策略等。

除此之外，安全管理中心还应该具有集中管控的能力，《规范》中规定要建立一条安全的信息传输路径，并对分布在网络中的安全设备或安全组件进行管控；对分散在各个设备上的审计数据进行收集汇总和集中分析，保证审计记录的留存时间；能对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理；能对网络中发生的各类安全事件进行识别、报警和分析。

安全管理中心推荐部署在运维管理网，使用带外管理的方式实现对网络安全设备的管理。将管理面网络与业务面网络分离，限制 IP 地址访问权限，关闭非安全访问协议（如 Telnet），提高安全管理的效率、可靠性和安全性。

3.6.3. 城轨云安全边界

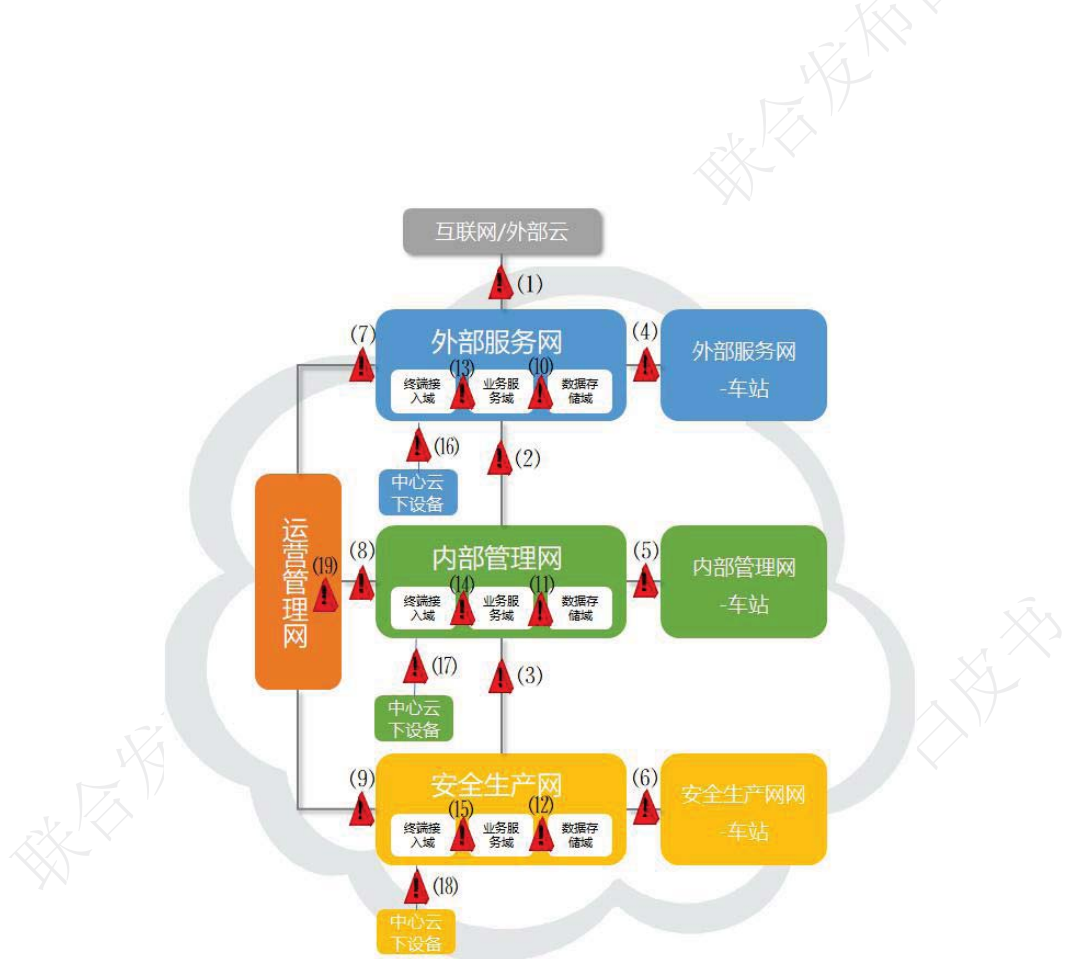
《智慧城市轨道交通 信息技术架构及网络安全规范 第 3 部分：网络安全》中，规定了城轨云的 14 个逻辑安全边界：

- 1) 外部服务网与互联网边界
- 2) 外部服务网内部区域边界
- 3) WLAN 系统边界
- 4) 外部服务网与内部管理网边界
- 5) 内部管理网内部区域边界

- 6) 内部管理网与安全生产网边界
- 7) 安全生产网内部区域边界
- 8) 安全生产网与信号系统边界
- 9) LTE 系统边界
- 10) 车站节点域边界
- 11) 终端接入边界
- 12) 运维管理网内部区域边界
- 13) 运维管理网与外部服务网、内部管理网、安全生产网的区域边界
- 14) 新建和既有系统边界

在系统实际部署中，有些逻辑安全边界是落到了同一个安全设备上。如“11. 安全生产网与信号系统边界”，“13. 新建和既有系统边界”和“14. LTE 系统边边界”，在安全生产网中都是经过非云接入交换机，用非云接入防火墙进行安全防护。下图展示了真实部署环境的物理边界。

城轨云物理边界示意：



其中列出的 19 个物理边界分别为：

- 1) 互联网边界：1
- 2) 外部服务网-内部管理网边界：2
- 3) 内部管理网-安全生产网边界：3
- 4) 中心云各网域-车站边界：4-6
- 5) 运维管理网-各业务网域边界：7-9
- 6) 各网域内的业务系统间边界：10-12
- 7) 各网域内的终端接入边界：13-15
- 8) 各网域内的云上-云下边界：16-18
- 9) 运维管理内区域边界：19

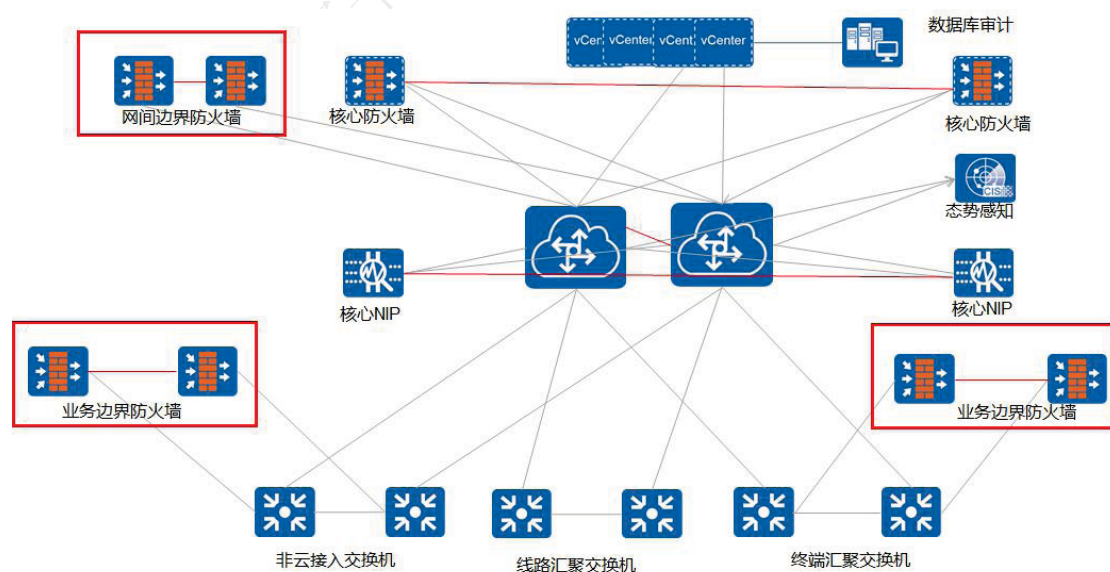
逻辑边界与物理边界的对应关系：

序号	协会规范（逻辑接口）	实际部署物理接口	备注
1	外部服务网与互联网边界	1	
2	外部服务网内部区域边界	10	
3	WLAN 系统边界	16, 18	WLAN 流量先汇到应用网络，

			再从各网域的云-非云边界上云
4	外部服务网与内部管理网边界	2	
5	内部管理网内部域边界	11	
6	内部管理网与安全生产网边界	3	
7	安全生产网内部区域边界	12	
8	安全生产网与信号系统边界	18	即安全生产网的云-非云边界
9	LTE 系统边界	18	即安全生产网的云-非云边界
10	车站节点域边界	4, 5, 6	
11	终端接入边界	13, 14, 15	
12	运维管理网内部区域边界	19	
13	运维管理网与外部服务网、内部管理网、安全生产网的区边界	7, 8, 9	
14	新建和既有系统边界	16, 17, 18	即各网域的云-非云边界

3.6.4. 信息安全部署框架

3.6.4.1. 安全生产网



边界	设备	备注
内部管理网/安全生产网边界	网间边界防火墙 *2	
安全生产网内部区域边界	核心防火墙 *2	
	核心 IPS *2	可包含网络防病毒功能
运维管理网/安全生产网边界	网管防火墙 *1	
车站节点域边界	防火墙 *2/每站 中心无设备	
终端接入边界	业务边界防火墙 *2	
	终端准入系统	部署在运维管理网
云-非云边界	业务边界防火墙 *2	
其它安全设备	数据库审计	
	态势感知	如全平台部署态势感知,可将主系统部署至运维管理网,本网仅保留探针

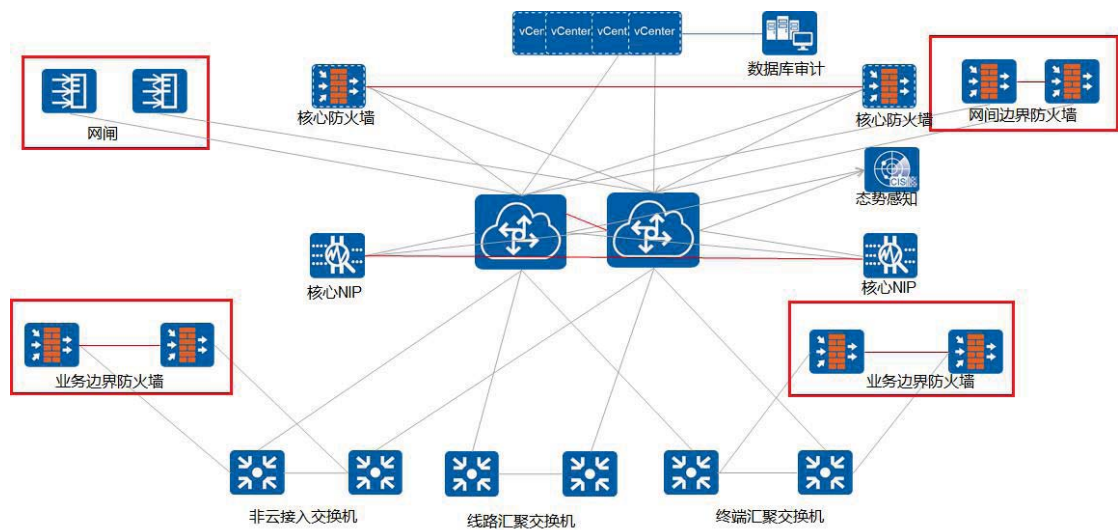
对于业务网域而言,网络中心是核心交换机,围绕核心交换机部署核心防火墙和核心 IPS,只要是经过核心交换机的网络流量均会通过核心防火墙和核心 IPS。这两类核心安全设备均要求支持虚拟化功能,可以配合云管理系统实现租户级别的安全防护与隔离能力,如虚拟防火墙等,在表中列为“安全生产网内部区域边界”。其中核心 IPS 还具有病毒墙功能,能够阻断病毒的传播

与其它网域通信时候,使用了边界火墙进行防护,这些网域边界包括:生产网-内管网、生产网(中心)-站段、生产网-运维管理网、生产网终端汇聚生产网非云接入。这些安全设备实现了网域间的通信网络防护与区域边界防护。

安全生产网内还部署了数据库审计设备用于计算环境防护,态势感知设备可满足网域内安全中心的需求。态势感知系统也可以部署在运维管理网,实现全网域的安全管理,在这种配置下,安全生产网内仅需设置探针功能即可。

运维管理网与安全生产网之间边界、虚拟化主机、车站业务边界除传统的安全防护之外,未来可考虑引入标记强制访问控制技术,用户只能访问到被标明由其访问的信息。

3.6.4.2.内部管理网

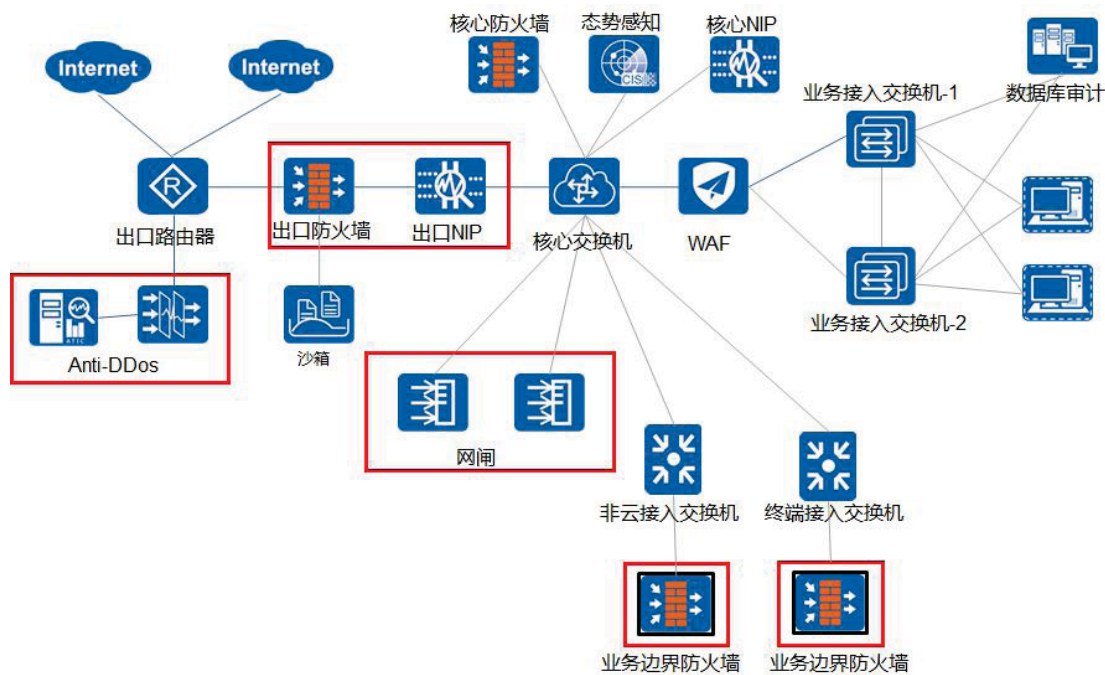


边界	设备	备注
内部管理网/安全生产网边界	网间边界防火墙 *2	
内部管理网/外部服务网边界	网闸 *2	
内部管理网内部区域边界	核心防火墙 *2	
	核心 IPS *2	可包含网络防病毒功能
运维管理网/内部管理网边界	网管防火墙 *1	
车站节点域边界	防火墙 *2/每站 中心无设备	内部管理网是否有车站节点需根据项目情况确定
终端接入边界	业务边界防火墙 *2	
	终端准入系统	部署在运维管理网
云-非云边界	业务边界防火墙 *2	内部管理网是否有非云系统需根据项目情况决定
其它安全设备	数据库审计	
	态势感知	如全平台部署态势感知,可将主系统部署至运维管理网,本网仅保留探针

与安全生产网设置类似, 内部管理网的核心防火墙+核心 IPS 具有租户级别的安全防护与

隔离能力，在表中列为“内部管理网内部区域边界”。其它如通信网络防护、区域边界防护、计算环境防护、安全管理中心功能，均与安全生产网类似。唯一的不同，是内部管理网和外部服务网之间，通过网闸设备进行物理隔离，而不是防火墙。

3.6.4.3.外部服务网



协会《规范》中并未对外部服务网的等保等级进行规定，网络需根据实际项目需要配置为单核心或双核心。安全设备的数量需适配网络配置。

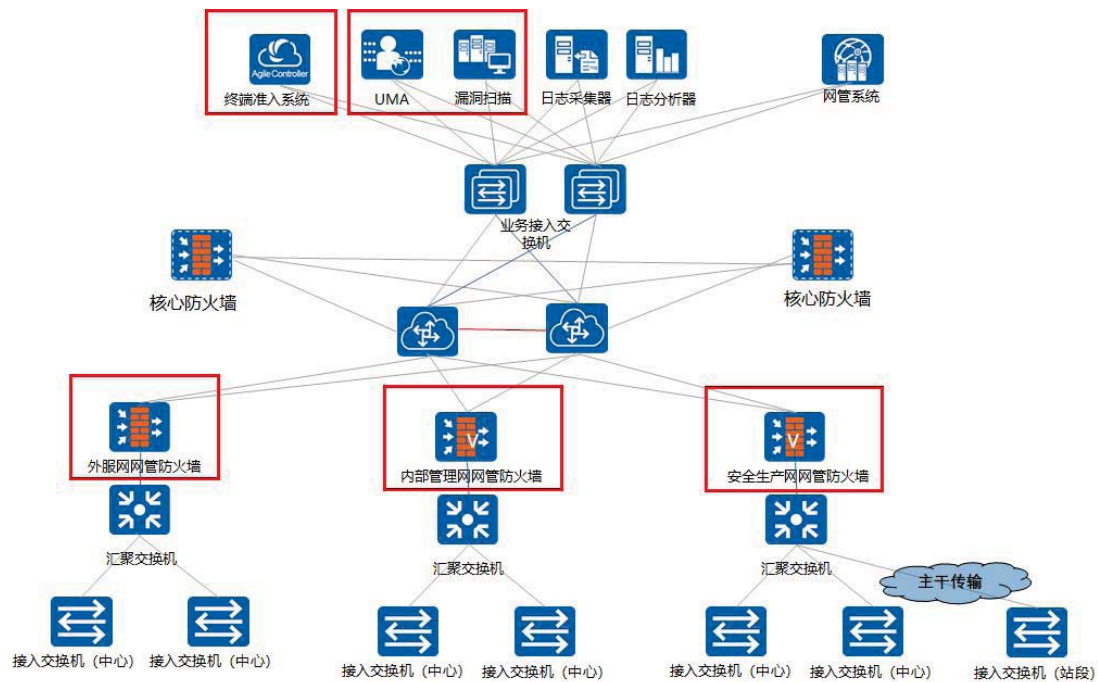
边界	设备	备注
外部服务网与互联网边界	出口防火墙	
	出口 IPS	
	沙箱	
	DDOS	
内部管理网/外部服务网边界	网闸 *2	
外部服务网网内部区域边界	核心防火墙	
	核心 IPS	可包含网络防病毒功能
运维管理网/安全生产网边界	网管防火墙 *1	

车站节点域边界	防火墙 *2/每站 中心无设备	
终端接入边界	业务边界防火墙 *1	
	终端准入系统	部署在运维管理网
云-非云边界	业务边界防火墙 *1	
其它安全设备	数据库审计	
	态势感知	如全平台部署态势感知,可将主系统部署至运维管理网,本网仅保留探针
	WAF	

外部服务网的核心防火墙与核心 IPS 具有租户级别的安全防护与隔离能力,在表中列为“外部服务网内部区域边界”。其它如通信网络防护、区域边界防护、计算环境防护、安全管理中心功能,与内部管理网类似。

外部服务网还有一个重要功能:与互联网进行通信,外部服务网在通往互联网的网络路径上部署了大量安全设备用于保证系统有足够的防护。这些安全设备包括:互联网出口防火墙、互联网出口 IPS、沙箱和 DDOS。除此之外,如果外部管理网需要承载网站,还可以增加 WAF (Web Application Firewall) 设备。

3.6.4.4.运维管理网



边界	设备	备注
运维管理网/各业务网边界	安全生产网防火墙*1	
	内部管理网防火墙*1	
	外部服务网防火墙*1	
运维管理网网内部区域边界	核心防火墙 *2	建议包含网络防病毒功能
其它安全设备	终端准入	
	运维审计堡垒机（UMA）	
	漏洞扫描	
	日志审计	

运维管理网部署了全网域的安全管理类和安全管控类设备，包括终端准入、运维审计堡垒机、漏洞扫描、日志审计等。态势感知系统根据需要，可以统一部署在运维管理网，也可以分别部署在各业务网域。

运维管理网与 3 个业务网域间使用防火墙进行隔离，可部署核心防火墙，建议包含网络防病毒功能。

3.6.5. 呼和浩特城轨云等保评测

安全等保测评的目的是通过对目标系统在安全技术及管理方面的测评，对目标系统的安全技术状态及安全管理状态做出初步判断，给出目标系统在安全技术及安全管理方面与其相应安全等级保护要求之间的差距。测评结论作为委托方进一步完善系统安全策略及安全技术防护措施的依据。

通过网络安全等级保护测评，一是掌握信息系统安全状态、排查系统安全隐患的薄弱环节、明确信息安全建设整改需求；二是能够衡量出信息系统安全保护措施是否符合网络安全的等级保护基本要求，是否具备了相应等级的安全保护能力；三是根据评测结果出具整改建议，指导系统运营、使用单位下一步的具体安全建设、整改工作，最终使系统达到国家安全等级保护的相关要求，避免相关安全风险事件的发生。三是根据评测结果出具整改建议，指导运营单位、使用单位深入开展安全建设以及整改工作，最终使系统达到国家安全等级保护的相关要求，避免相关安全风险事件的发生。

呼和浩特城轨云作为全国首个多线路多业务综合云平台，通过解读等保 2.0 标准以及协会《规范》中网络安全相关要求，确立呼和浩特城轨云等保评测原则，开展等保评测工作。通过总结网络安全等级保护评测实践经验，指导行业内云平台等保评测工作。

3.6.5.1. 等保评测原则

3.6.5.1.1. 等保依据

1. GB/T17859-1999 《信息安全技术 计算机信息系统安全保护等级划分准则》
2. GB/T22239-2019 《信息安全技术 网络安全等级保护基本要求》
3. GB/T284880-2019 《信息安全技术 网络安全等级保护测评要求》
4. GB/T28449-2018 《信息安全技术 网络安全等级保护测评过程指南》
5. GB/T20984-2007 《信息安全技术 信息安全风险评估模型》

3.6.5.1.2. 定级原则

1. 遵循“系统自保、平台统保、边界防护、等保达标、安全确保”的策略，以网络安全等级保护为基础，分级分类建立应用系统的安全保护措施。
2. 业务系统的安全应由应用系统自身安全机制和云平台安全机制协同保障，云平台应具备最高支持，应用系统达到网络安全等级保护第三级的能力。
3. 安全生产网应按照等保三级建设，内部管理网应按照等保二级建设，外部服务网按各应用所需的级别建设，并确保达到相应等级的实际安全保护效果。

4. 由于操作系统、数据库均由业务系统提供，因此云平台与业务系统安全边界设定在操作系统层。操作系统以下的物理环境、网络安全、边界防护由云平台提供保护，操作系统及以上的身份识别、访问控制、资源控制主要有业务系统负责，云平台配合实现其中部分要求。
5. 云平台提供统一安全管理，可与业务系统提供的安全管理功能组合使用，但至少保证有一方提供可用的安全管理功能。

3.6.5.2. 等保定级

3.6.5.2.1. 安全生产网安全保护等级的确定

一、 业务信息安全保护等级的确定

1. 业务信息描述

安全生产网业务主要包含：综合监控系统、自动售检票系统、乘客信息系统、门禁系统、公务电话系统、通信集中告警系统、列车自动监控系统 and 数据挖掘系统等。

2. 业务信息受到破坏时所侵害客体的确定（侵害的客体包括：1 国家安全，2 社会秩序和公共利益，3 公民、法人和其他组织的合法权益等共三个客体）

该业务信息遭到破坏后，所侵害的客体是公民、法人和其他组织的合法权益。

侵害的客观方面（客观方面是指定级对象的具体侵害行为，侵害形式以及对客体的造成的侵害结果）表现为：一旦信息系统的业务信息遭到入侵、修改、增加、删除等不明侵害（形式可以包括丢失、破坏、损坏等），会对公民、法人和其他组织的合法权益造成影响和损害，可以表现为：影响正常工作的开展、导致业务能力下降、造成不良影响、引起法律纠纷等。

3. 信息受到破坏后对侵害客体的侵害程度（即上述分析结果的表现程度）

上述结果的程度表现为严重损害，即工作职能收到严重影响、业务能力显著下降、出现较严重的法律问题、较大范围的不良影响等。

4. 确定业务信息安全等级

查《定级指南》表 2 知，业务信息安全保护等级为第三级。

业务信息安全被破坏时所侵害的客体	对相应客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第二级

社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

二、系统服务安全保护等级的确定

1、系统服务描述

该系统属于为国计民生、经济建设等提供服务的信息系统，其服务范围为全自治区范围内的普通公民、法人等。

2、信息受到破坏后对侵害客体的侵害程度（即上述分析结果的表现程度）

上述结果的程度表现为：对社会秩序和公共利益造成严重损害，即会出现较大范围的社会不良影响和较大程度的公共利益的损害等。

3、确定系统服务安全等级

查《定级指南》表3知，由于侵害的客体有两个，侵害的程度也有两个，则业务信息安全保护等级为第三级。

系统服务被破坏时所侵害的客体	对相应客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第三级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

三、安全保护等级的确定

信息系统的安全保护等级由业务信息安全等级和系统服务安全等级的较高者决定。所以，安全生产网安全保护等级为第三级。

信息系统名称	安全保护等级	业务信息安全等级	系统服务安全等级
安全生产网	第三级	第三级	第三级

3.6.5.2.2. 内部服务网安全保护等级的确定

一、业务信息安全保护等级的确定

1. 业务信息描述

运营生产系统业务主要包含：资产管理一体化平台、运营一体化平台、协同办公一体化平台等等。

2. 业务信息受到破坏时所侵害客体的确定（侵害的客体包括：1 国家安全，2 社会秩序和公共利益，3 公民、法人和其他组织的合法权益等共三个客体）

该业务信息遭到破坏后，所侵害的客体是公民、法人和其他组织的合法权益。

侵害的客观方面（客观方面是指定级对象的具体侵害行为，侵害形式以及对客体的造成的侵害结果）表现为：一旦信息系统的业务信息遭到入侵、修改、增加、删除等不明侵害（形式可以包括丢失、破坏、损坏等），会对公民、法人和其他组织的合法权益造成影响和损害，可以表现为：影响正常工作的开展、导致业务能力下降、造成不良影响、引起法律纠纷等。

3. 信息受到破坏后对侵害客体的侵害程度（即上述分析结果的表现程度）

上述结果的程度表现为严重损害，即工作职能收到严重影响、业务能力显著下降、出现较严重的法律问题、较大范围的不良影响等。

4. 确定业务信息安全等级

查《定级指南》表 2 知，业务信息安全保护等级为第二级。

业务信息安全被破坏时所侵害的客体	对相应客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第二级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

二、 统服务安全保护等级的确定

1. 系统服务描述

该系统属于为国计民生、经济建设等提供服务的信息系统，其服务范围为全自治区范围内的普通公民、法人等。

2. 确定系统服务安全等级

查《定级指南》表 3 知，由于侵害的客体有两个，侵害的程度也有两个，则业务信息安全保护等级为第二级。

系统服务被破坏时所侵害的客体	对相应客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第三级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

三、 安全保护等级的确定

信息系统的安全保护等级由业务信息安全等级和系统服务安全等级中的较高者决定。所以，内部管理网安全保护等级为第二级。

信息系统名称	安全保护等级	业务信息安全等级	系统服务安全等级
内部管理网	第三级	第三级	第三级

3.6.5.2.3. 外部管理网安全保护等级的确定

一、 业务信息安全保护等级的确定

1. 业务信息描述

运营生产系统业务主要包含：邮件系统、外部网站、互联网购票子系统手机 APP 平台。

2. 业务信息受到破坏时所侵害客体的确定（侵害的客体包括：1 国家安全，2 社会秩序和公共利益，3 公民、法人和其他组织的合法权益等共三个客体）

该业务信息遭到破坏后，所侵害的客体是公民、法人和其他组织的合法权益。

侵害的客观方面（客观方面是指定级对象的具体侵害行为，侵害形式以及对客体的造成的侵害结果）表现为：一旦信息系统的业务信息遭到入侵、修改、增加、删除等不明侵害（形式可以包括丢失、破坏、损坏等），会对公民、法人和其他组织的合法权益造成影响和损害，可以表现为：影响正常工作的开展、导致业务能力下降、造成不良影响、引起法律纠纷等。

3. 信息受到破坏后对侵害客体的侵害程度（即上述分析结果的表现程度）

上述结果的程度表现为严重损害，即工作职能收到严重影响，业务能力显著下降，出现较严重的法律问题，较大范围的不良影响等。

4. 确定业务信息安全等级

查《定级指南》表 2 知，业务信息安全保护等级为第三级。

业务信息安全被破坏时所侵害的客体	对相应客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第二级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

二、系统服务安全保护等级的确定

1. 系统服务描述

该系统属于为国计民生、经济建设等提供服务的信息系统，其服务范围为全自治区范围内的普通公民、法人等。

2. 确定系统服务安全等级

查《定级指南》表 3 知，由于侵害的客体有两个，侵害的程度也有两个，则业务信息安全保护等级为第三级。

系统服务被破坏时所侵害的客体	对相应客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第三级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

三、安全保护等级的确定

信息系统的安全保护等级由业务信息安全等级和系统服务安全等级的较高者决定。所以，外部服务网安全保护等级为第三级。

信息系统名称	安全保护等级	业务信息安全等级	系统服务安全等级
外部服务网	第三级	第三级	第三级

3.6.5.2.4. 运维管理网安全保护等级的确定

一、 业务信息安全保护等级的确定

1. 业务信息描述

运维管理网系统业务主要包含：主要承载网络及 IT 设备带外业务以及安全设备（Esight、Elog、UMA 等）。

2. 业务信息受到破坏时所侵害客体的确定（侵害的客体包括：1 国家安全，2 社会秩序和公共利益，3 公民、法人和其他组织的合法权益等共三个客体）

该业务信息遭到破坏后，所侵害的客体是公民、法人和其他组织的合法权益。

侵害的客观方面（客观方面是指定级对象的具体侵害行为，侵害形式以及对客体的造成的侵害结果）表现为：一旦信息系统的业务信息遭到入侵、修改、增加、删除等不明侵害（形式可以包括丢失、破坏、损坏等），会对公民、法人和其他组织的合法权益造成影响和损害，可以表现为：影响正常工作的开展、导致业务能力下降、造成不良影响、引起法律纠纷等。

3. 信息受到破坏后对侵害客体的侵害程度（即上述分析的结果的表现程度）

上述结果的程度表现为严重损害，即工作职能收到严重影响，业务能力显著下降，出现较严重的法律问题，较大范围的不良影响等。

4. 确定业务信息安全等级

查《定级指南》表 2 知，业务信息安全保护等级为第二级。

业务信息安全被破坏时所侵害的客体	对相应客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第二级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

二、 系统服务安全保护等级的确定

1. 系统服务描述

该系统属于为国计民生、经济建设等提供服务的信息系统，其服务范围为全自治区范围内的普通公民、法人等。

2. 确定系统服务安全等级

查《定级指南》表3知，由于侵害的客体有两个，侵害的程度也有两个，则业务信息安全保护等级为第二级。

系统服务被破坏时所侵害的客体	对相应客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第三级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

三、 安全保护等级的确定

信息系统的安全保护等级由业务信息安全等级和系统服务安全等级的较高者决定。所以，运维管理网安全保护等级为第二级。

信息系统名称	安全保护等级	业务信息安全等级	系统服务安全等级
运维管理网	二级	第二级	第二级

3.6.5.3.等保测评流程

等保测评活动大致分为测评准备活动、现场测评活动、报告编制活动。



通过对信息系统进行等级符合性检验，最终出具等级测评报告，可以帮助信息系统运营、使用单位发现信息系统的安全防护能力与国家等级保护要求之间的差距，发现信息系统存在

的安全隐患和薄弱环节，指导系统运营、使用单位下一步的具体安全建设、整改工作，最终使系统达到国家等级保护的相关要求，避免相关安全风险事件的发生。

《网络安全等级保护测评报告》，将从安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理等各个单元层面以及整体层面明确提出被测信息系统存在的安全隐患和薄弱环节。同时，采用风险分析的方法分析信息系统网络安全等级保护测评结果中存在的安全问题可能对信息系统安全造成的影响。

报告将针对信息系统存在的安全问题，给出相应的改进建议。为信息系统安全建设整改提供安全理论依据，为决策者制定安全策略、构架安全体系以及确定有效的安全措施、选择可靠的安全产品、建设全面的安全防护层次提供规范的指导。

3.6.5.3.1. 测评准备活动

测评准备活动的目标是顺利启动测评项目，收集定级对象相关资料，准备测评所需资料，为编制测评方案打下良好的基础。

- 等级测评项目启动

项目启动实施过程：在工作启动任务中，测评机构组建等级测评项目组，获取测评委托单位及定级对象的基本情况，从基本资料、人员、计划安排等方面为整个等级测评项目的实施做好充分准备。

项目启动工作产品：项目计划书。

- 信息收集和分析

信息收集和分析实施过程：测评机构通过查阅被测定级对象已有资料或使用系统调查表格的方式，了解整个系统的构成和保护情况以及责任部门相关情况，为编写测评方案、开展现场测评和安全评估工作奠定基础。

信息收集和分析工作产品：填好的调查表格。

- 工具和表单准备

工具和表单准备实施过程：测评项目组成员在进行现场测评之前，应熟悉被测定级对象、调试测评工具、准备各种表单等。

工具和表单准备工作产品：选用的测评工具清单，打印的各类表单。

3.6.5.3.2. 现场测评活动

现场测评活动通过与测评委托单位进行沟通和协调，为现场测评的顺利开展打下良好基础，依据测评方案实施现场测评工作，将测评方案和测评方法等内容具体落实到现场测评活动中。现场测评工作应取得报告编制活动所需的、足够的证据和资料。

现场测评活动包括现场测评准备、现场测评和结果记录、结果确认和资料归还三项主要任务。

- 现场测评准备

现场测评准备实施过程：测评委托单位对风险告知书签字确认，了解测评过程中存在的安全风险，做好相应的应急和备份工作。测评委托单位签署现场测评授权书。召开测评现场首次会，测评机构介绍现场测评工作安排，相关方对测评计划和测评方案中的测评内容和方法等进行沟通。测评相关方确认现场测评需要的各种资源，包括测评配合人员和需要提供的测评环境等。现场测评工作正式开启。

现场测评准备输出产品：会议记录、测评方案、现场测评工作计划和风险告知书、现场测评授权书。

- 现场测评和结果记录

现场测评和结果记录实施过程：现场测评一般包括访谈、文档审查、配置检查、测试和实地察看五个方面。

访谈：测评人员与被测系统有关人员进行交流、讨论等活动，获取相关证据，了解有关信息。

输出产品：技术和管理安全测评的测评结果记录。

文档审查：被测评单位人员将调查表格中提供的所有文档准备充分，测评人员根据GB/T 22239中规定的制度、策略、操作规程等文档是否齐备；检查是否有完整的制度执行情况记录，如机房出入登记记录、电子记录、高等级系统的关键设备的使用登记记录等；检查安全策略以及技术相关文档是否明确说明相关技术要求实现方式；对上述文档进行审核与分析，检查他们的完整性和这些文件之间的内部一致性。

输出产品：技术和管理安全测评的测评结果记录。

实地察看：根据被测定级对象的实际情况，测评人员到系统运行现场通过实地的观察人员行为、技术设施和物理环境状况判断人员的安全意识、业务操作、管理程序和系统物理环境等方面的安全情况，测评其是否符合相应等级的安全要求。

实地察看输出产品：技术安全和管理安全测评结果记录。

配置检查：根据测评结果记录表格内容，利用上机验证的方式检查应用系统、主机系统、数据库系统以及各设备的配置是否正确，是否与文档、相关设备和部件保持一致，对文档审核的内容进行核实（包括日志审计等）；如果系统在输入无效命令时不能完成其功能，应测试其是否对无效命令进行错误处理；针对网络连接，应对连接规则进行验证。

配置检查输出产品：技术安全测评结果记录。

测试：根据测评指导书，利用技术工具对系统进行测试，包括基于网络探测和基于主机审计的漏洞扫描、渗透性测试。

测试输出产品：技术安全测评结果记录、测试完成后的电子输出记录、备份的测试结果文件。

- 结果确认和资料归还

结果确认和资料归还实施过程：测评人员在现场测评完成之后，应首先汇总现场测评的测评记录，对漏掉和需要进一步验证的内容实施补充测评。双方召开测评现场结束会，测评双方对测评过程中得到的证据源记录进行现场沟通和确认。测评机构归还测评过程中借阅的所有文档资料，并由测评委托单位文档资料提供者签字确认。

结果确认和资料归还输出产品：经过测评委托单位确认的测评证据和证据源记录。

3.6.5.3.3. 报告编制活动

现场测评工作结束后，测评机构应对现场测评获得的测评结果（或称测评证据）进行汇总分析，形成等级测评结论，并编制测评报告。

测评人员在初步判定单项测评结果后，还需进行单元测评结果判定、整体测评、系统安全保障评估。经过整体测评后，有的单项测评结果可能会有所变化，需进一步修订单项测评结果，而后针对安全问题进行风险评估，形成等级测评结论。分析与报告编制活动包括单项测评结果判定、单元测评结果判定、整体测评、系统安全保障评估、安全问题风险评估、等级测评结论形成和测评报告编制七项主要任务。

报告编制活动实施过程：测评机构编制测评报告，并提交给测评委托单位进行验收评审，测评委托单位确认，项目结束。

3.6.5.3.4. 等保组织及职责



建设单位作为被测评单位，各阶段责任如下：

1、测评准备阶段

- 1) 向测评机构介绍本单位的信息化建设状况与发展情况。
- 2) 提供测评机构需要的相关资料。
- 3) 为测评人员的信息收集工作提供支持和协调。
- 4) 准确填写调查表格。
- 5) 根据被测定级对象的具体情况，如业务运行高峰期、网络布置情况等，为测评时间安排提供适宜的建议。
- 6) 制定应急预案。
- 7) 作为云租户的测评委托单位职责还应包括：负责与云服务商沟通与协调，为测评人员的信息收集工作提供协助。

2、方案编制阶段

- 1) 为测评机构完成测评方案提供有关信息和资料。
- 2) 评审和确认测评方案文本。
- 3) 评审和确认测评机构提供的风险规避实施方案。
- 4) 若确定不在生产环境开展测评，则部署配置与生产环境各项安全配置相同的备份环境、生产验证环境或测试环境作为测试环境。

3、现场测评阶段

- 1) 测评前备份系统和数据，并了解测评工作基本情况。
- 2) 协助测评机构获得现场测评授权。
- 3) 安排测评配合人员，配合测评工作的开展。
- 4) 对风险告知书进行签字确认。
- 5) 配合人员如实回答测评人员的问询，对某些需要验证的内容上机进行操作。
- 6) 配合人员协助测评人员实施工具测试并提供有效建议，降低安全测评对系统运行的影响。
- 5) 配合人员协助测评人员完成业务相关内容的问询、验证和测试。
- 6) 配合人员对测评证据和证据源进行确认。
- 7) 配合人员确认测试后被测设备状态完好。
- 8) 作为云租户的测评委托单位职责还应包括：协助测评机构获得云平台现场测评授权、负责协调云服务商配合测评或提供云计算平台等级测评报告等。

4、报告编制阶段

- 1) 签收测评报告。
- 2) 向分管公安机关备案测评报告。

测评机构人员职责：

项目负责人：负责项目具体实施和管理，制定项目实施计划，掌握项目的每个实施过程，解决项目实施中出现的各种具体问题，项目变化的管理，风险管理，与客户进行及时有效的沟通，定期向用户反馈项目进展情况。

技术测试组：负责项目具体的技术测试实施，如网络平台测试、系统平台测试、业务应用测试等，定期向测评负责人反馈技术测试进展情况。

管理评估组：负责项目具体的安全管理的评估，实施现场访谈、制度核查、执行记录查阅等，定期向测评负责人反馈管理评估进展情况。

工具测试组：负责汇总技术测试中发现的安全隐患，针对发现的安全漏洞，选择适当的

攻击工具及方法，模拟入侵行为。

质量监督人：对项目实施全过程的质量监控，动态监控质量体系执行情况，对违反质量管理规范的情况提出改进或否决意见，及时出具质量监控报告或意见。

3.6.5.4. 注意事项

1. 网络安全等级保护包括安全管理机构，其主要为主观行为，如成立安全领导小组，设立网络安全管理的职能部门，提供外部人员访问系统的管理机制等，需要建设单位前期注重网络安全管理制度的完善，加强网络安全职能部门之间的协助；
2. 对安全计算环境（主机）的访问要做到多重鉴别技术的组合，以达到对用户身份的高度识别，修改默认易猜解的默认管理账户名；
3. 网络安全设备需定期进行审计、扫描和备份等主动性保护动作，确保数据能够及时得到分析和保存。

3.7. 云平台应用部署实例

3.7.1. ATS、ISCS 部署网络结构优化

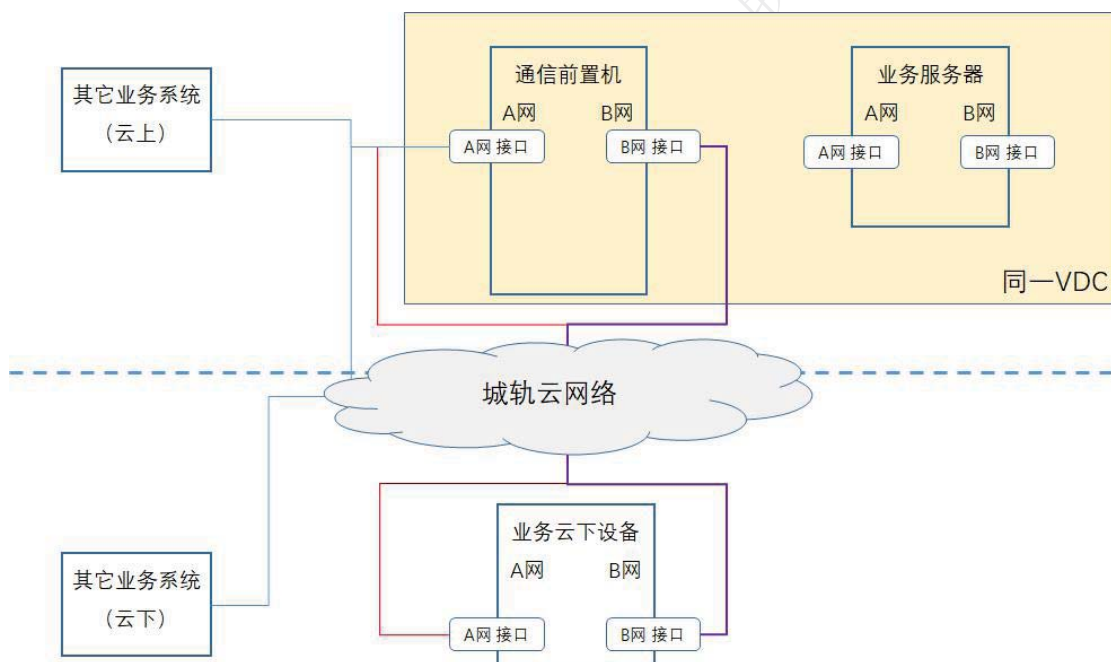
ATS 和 ISCS 业务系统均使用通信前置机与其他系统通信，在传统部署模式下，会使用多块网卡实现与其他业务系统通信，即为每一个需通信的业务系统配置一块独立网卡。

呼和浩特城轨云平台的网络结构与传统城轨网络存在着较大差异，包括：

- 1) 部署在云平台中的各业务系统多数以虚拟机形式承载，虚拟机各网卡最终均由物理网卡执行流量转发，因此，传统城轨模式下通过增加网卡来提高可靠性的方式，在云平台中意义有限，可将多块角色相同的网卡合并，使用一块虚拟网卡对外通信，由云平台底层物理架构确保通信的可靠性。
- 2) 由于云平台在底层就保证了链路的冗余，云上系统间通信完全可以采用单网通信。

为了保证与云下系统 AB 网兼容性，云上系统依然需要保持 AB 网的结构。在优化过网络结构后，推荐采用如下架构：

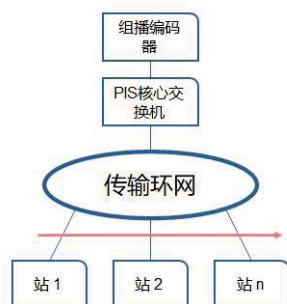
云上主机（通信前置机、业务服务器）配置 2 块网卡。A 网接口为主网卡，除了接 A 网设备之外，还需要接云上云下其他系统。B 网接口仅和云下 B 网设备通信。



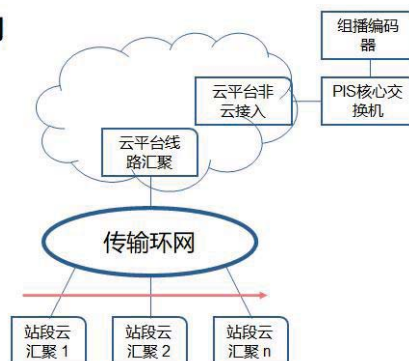
3.7.2. 云上组播结构优化

城轨云平台内部使用的是 SDN 网络，如果 PIS 或 CCTV 部署在中心，则需要城轨云网络支持组播协议（IGMP、PIM-SM、PIM-DM），这样才能实现 PIS 或 CCTV 向多个站段同时发送视频流的功能。

传统组网



云平台组网



组播网络可能会出现占用的带宽会随着站点增加而线性增长的问题，在呼和浩特城轨云的实践中，PIS 系统站段设备独立成段，网关落在站段。组播协议会认为每一个站段云节点都是一个组播节点，送至传输环网的组播流量会有一个 n 倍乘的关系。即如果线路上有 10 个组播节点，会传输 10X 的组播视频，如果有 20 个组播节点，会传输 20X 的组播视频，占用的带宽会随着站点增加而线性增长。

在呼和浩特环境下，PIS 系统一路组播大约是 5Mbps，按单线不超过 20 个站段节点的规模计算，稳定的一路组播流量大约在 100Mbps 左右。但是在实际应用中，PIS 系统会出现组播视频流带宽波动的情况，突发流量带宽可能会突破 50Mbps，总流量则会超过 1Gbps，尽管

这种峰值维持时间及短，但仍会引起站段接收端画面马赛克的问题，通过实践，这个问题可以通过增大传输系统突发带宽设置缓解。

在后续线路中，需要云平台集成商提前测试验证，是否有其它解决问题的思路（如参考 PIS、CCTV 独立组网方式）。如后续测试证明，基于城轨云环境这种组播随着站点增加而线性增长的问题会一直存在，则需要在传输带宽规划中考虑组播突发带宽增大的情况。若传输物理带宽不足，可以考虑传输环网使用 OTN 系统。

3.7.3. ATS 系统在云上可用性指标的计算

ATS 系统要求云平台的可用性指标为 99.999%，可用性计算应是基于安全功能及安全功能涉及的设备。本白皮书中，使用下发临时限速功能示例如何计算 ATS 可用性指标。

1) 系统可用性计算公式

冗余系统采用马尔可夫模型计算，冗余单元又可以分为主备用和负载分担两种。下面是这两种冗余方式的计算公式。

2) N+1 主备用的可用性计算公式

$$A = 1 - \{C \times [1 - a^N \times (N + 1 - N \times a)] \div N + (1 - C) \times (1 - a^N) \div N\}$$

3) N+1 负载分担的可用性计算公式

$$A = 1 - \{C_A \times [1 - a^N \times (N + 1 - N \times a)] \div N + (1 - C_A) \times (1 - a^{N+1}) \div (N + 1)\}$$

- A: 1:N 冗余系统的可用度
- C: 倒换率—成功倒换的概率

$C_A \times C_S$ —主备用

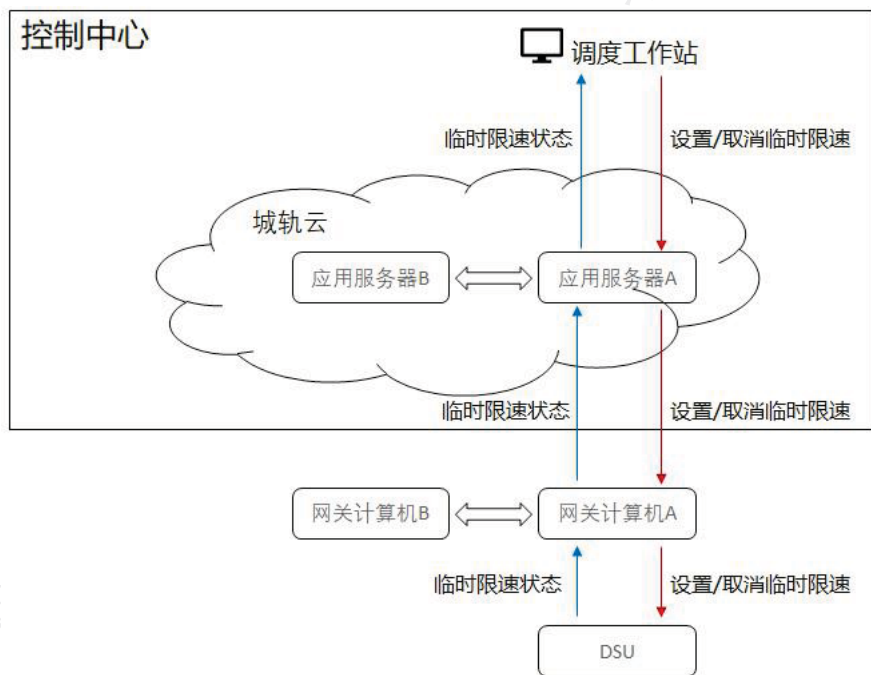
C_A —负荷分担

- C_A : 主用侧的故障检测率
- C_S : 备用侧的故障检测率
- a: N+1 个单元中每个单元的可用度 ($MTBF / (MTBF + MTTR)$)

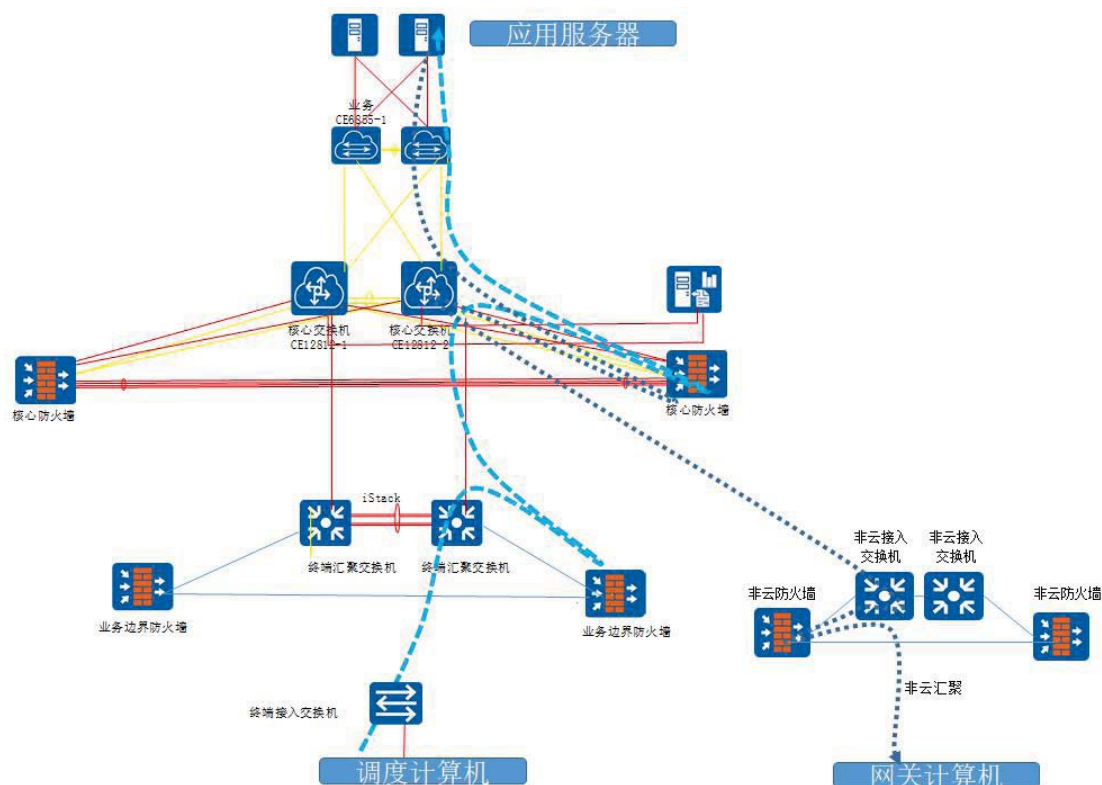
根据最后可用性结果就可以计算得到停机时间指标:

停机时间 $D_i = (60 \times 24 \times 365) \times (1 - A)$ 分钟 / 年

4) ATS 安全功能（临时限速）业务数据流向图



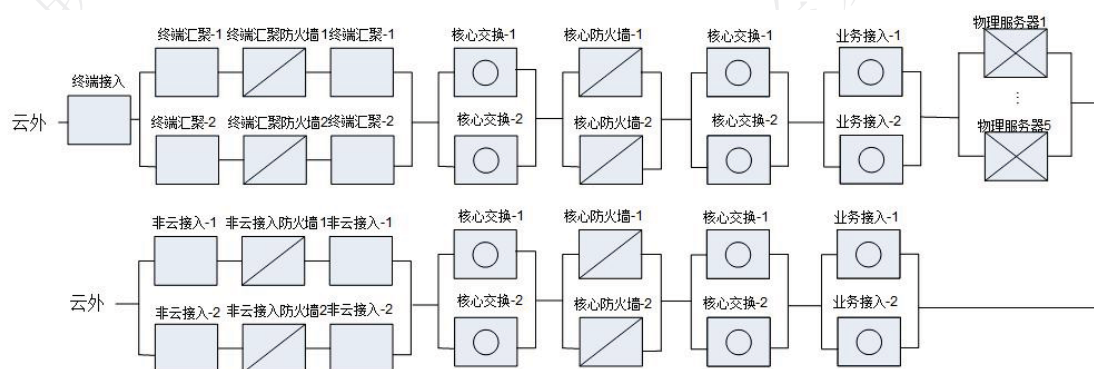
以呼和浩特云平台为例，上述数据流向在实际平台上的数据流动方式为：



- 1) 调度计算机使用物理工作站，通过终端接入交换机至终端汇聚设备（汇聚交换机及汇聚防火墙）后，进入进城轨云平台。

- 2) 去往应用服务器的通信首先经过核心交换机和核心防火墙，再通过业务接入交换机到达应用服务器所在的区域。
- 3) 云平台使用了虚拟化技术，应用服务器系统安装在云主机上，云主机可在多个物理服务器上迁移。这样能确保系统有更高的可用性。在呼和浩特云的实践 ATS 系统分配的资源池中包含 5 台物理服务器，物理服务器之间的关系是 N+1 主备用方式，计算可用度也是使用 N+1 的模型，这比传统服务器的 1+1 冗余要更稳定可靠。
- 4) 城轨云平台通过非云接入交换机与信号系统的云下网关计算机相连。网络通信从应用服务器出发，经过云平台业务接入交换机到达核心设备（核心交换机、核心防火墙及核心入侵检测防御），再经过非云接入交换机和非云接入防火墙。
- 5) 除了终端接入交换机是单机之外，其它网络设备均采用 1+1 冗余设置。除核心交换机使用的是负载分担模式外，其它网络设备均采用的是主备模式。

根据网络流向图生成的 RBD 框图见下：



网元设备指标及系统可用性计算：

各网元（交换机、防火墙、服务器等）的基本设备指标（即包括失效时间、MTBF、MTTR、可用性等），需要由设备厂商提供。作为基础输入数据，需要由设备厂商提供。

以呼和浩特城轨云平台为例，此路径上的设备指标见下表，MTTR 数值为厂家给出的典型场景下的统计值。

	失效时间 (分钟/年)	MTBF (年)	MTTR (小时)	可用性
终端接入交换机	3.05	39.31	2	99.99941920%
终端汇聚交换机	2.97	40.4	2	99.99943480%
终端边界防火墙	2.53	23.67	1	99.99957819%
核心交换机	1.79	33.52	1	99.99965939%

核心防火墙	0.87	34.37	1	99.99983400%
业务接入交换机	2.11	48.83	2	99.99959816%
物理服务器	2.3	26.3	1	99.99956650%
非云接入交换机	2.97	40.4	2	99.99943480%
非云边界防火墙	0.97	30.89	1	99.99981500%

计算在通信路径上各网元冗余后可用性指标：

	C	n	单元可用性 a	冗余后可用性 a	冗余关系
终端接入交换机	N/A	N/A	99.99941920%	99.99941920%	无
终端汇聚交换机	0.95	1	99.99943480%	99.99994348%	n+1 主备
终端边界防火墙	0.95	1	99.99957819%	99.99997891%	n+1 主备
终端汇聚交换机	0.95	1	99.99943480%	99.99997174%	n+1 主备
核心交换机	0.95	1	99.99965939%	99.99998297%	负载分担
核心防火墙	0.95	1	99.99983400%	99.99999170%	n+1 主备
核心交换机	0.95	1	99.99965939%	99.99998297%	负载分担
业务接入交换机	0.95	1	99.99959816%	99.99997991%	n+1 主备
物理服务器	0.95	4	99.99956650%	99.99997832%	n+1 主备
业务接入交换机	0.95	1	99.99959816%	99.99997991%	n+1 主备
核心交换机	0.95	1	99.99965939%	99.99998297%	负载分担
核心防火墙	0.95	1	99.99983400%	99.99999170%	n+1 主备
核心交换机	0.95	1	99.99965939%	99.99998297%	负载分担
非云接入交换机	0.95	1	99.99943480%	99.99997174%	n+1 主备
非云接入防火墙	0.95	1	99.99981500%	99.99999075%	n+1 主备
非云接入交换机	0.95	1	99.99943480%	99.99997174%	n+1 主备

倒换率按照 95%计算，MTTR 按 1 小时计算（现场有备件）

- 系统可用性 $A = \prod_{n=1}^{16} a_n = 99.999101\%$
- $MTBF = A \times MTTR \div (1-A) \div 365 \div 24 = 12.7$ （年）
- $DT = (1-A) \times 365 \times 24 \times 60 = 4.73$ （分钟）

3.7.4. ATS 上云的 SIL 等级合规方案

SIL（Safety Integrity Level，安全完整性等级）技术标准是由国际电工委员会（IEC）首先颁布制定，用于量化危险操作的安全性能要求。有四个 SIL 级别（1-4），较高的 SIL 水平意味着更大的过程危害，需要更高级别的保护。

跟轨道交通相关的安全标准主要是包括三个：EN50126、EN50128、EN50129。其中 EN50126 定义了系统的 RAMS（reliability、availability、maintainability 和 safety），即可靠性、可用性、可维护性和安全性。EN50128 对控制和轨道交通相关的防护系统的软件进行了安全完善度等级(SIL)的划分。EN50129 引入安全生命周期概念，对于安全相关系统的安全部分进行全程的安全评估和验证。

信号 ATS 系统有 SIL2 安全等级要求，需要评估在城轨云的环境下信号 ATS 系统的 SIL 等级合规方案及实际落地的最佳工程实践。

信号 ATS 系统可在云上部署的部分包括：应用服务器、数据库服务器（裸金属）、通信前置机、调度工作站（云桌面）、时刻表编辑工作站（云桌面）、运行图显示工作站（云桌面）。

现阶段信号 ATS 系统涉安功能包括但不限于：强扳道岔、计轴复位、临时限速设置与取消、确认临时限速、确认雨雪模式。

以呼和浩特城轨云平台上承载的交控科技 ATS 系统为例，从上一节的业务数据流向图可以看出，以上列出的涉安功能均由调度工作站执行，通过应用服务器透传至网关计算机，再由网关计算机传至 ATC 网内相应的单元。在安全功能的执行过程中，安全功能的执行均在调度工作站上完成。只需要明确调度工作站上的系统是否符合 SIL2 安全等级合规即可。

传统调度工作站的系统结构：硬件 – 操作系统 – 应用软件，而部署在云桌面上的系统结构：硬件 – 云平台 – 操作系统 – 应用软件。即需要云平台证明，因为增加这一层，不会降低上层应用的安全完整性等级。

	方案	适用条件及限制
云平台过相关安全认证	桌面云系统通过 SIL 安全认证	具有普适性，可扩展至控制系统上云（如连锁）的场景
云平台提供相关 FMECA 报告	桌面云平台提供其内部的故障模式、影响及危害分析报告，供	须尽量穷举故障模式并分析其影响及危害，确保故障导向安全侧。与传统部署方式相

	安全机构验证	比，云桌面部署不会降低系统安全性
改变部署模式	将调度工作站部署在云下，采用物理机部署方式	云平台仅承载非安全功能。云下工作站 IP 段与云上工作站 IP 须在不同网段

如云平台厂商能提供桌面云系统 SIL 安全认证证书，或能提供 FEMCA 报告并配合安全机构通过 ATS 系统安全认证，那么可将调度工作站部署在桌面云平台上。如因时间或其它条件所限制，可将调度工作站部署在云下，即采用传统方式部署。这样即可满足 ATS 系统 SIL2 认证要求。

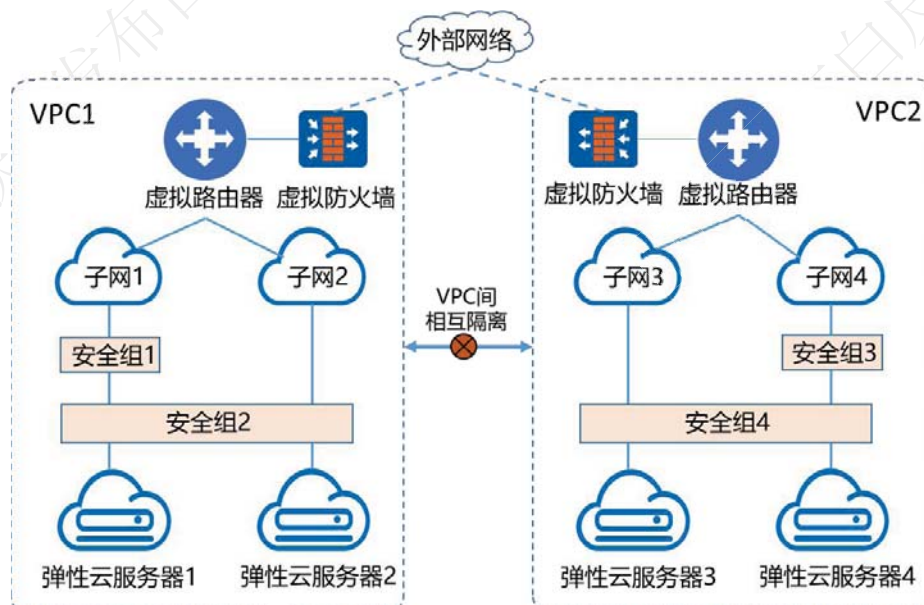
如将调度工作站部署在云下，须提前做好网络规划。须将云上、云下工作站的 IP 段分开。平台无法实现同一网段内部分主机在云上，部分主机在云下的部署方式。后期再调整 IP 地址可能会导致整体数据更新。

呼和浩特城轨云平台，采用的是物理机部署模式。调度工作站部署在云下，采用上架服务器与瘦客户端的模式。如果现场条件允许，也可以直接采用传统工作站方式部署。传统工作站部署方式有更好的用户体验。

3.7.5. 业务系统互联关系

城轨云平台是承载多专业多线路的统一平台，业务系统之间需要做到严格的网络管控，平台内各业务系统间仅运行接口服务器（或通信前置机等）通信，且对于信号系统 ATS、综合监控的冗余网络，需要做到专业内部冗余网络之间隔离。

为保障各业务系统通信安全，云平台为各专业线路级 VDC 设置对应 VPC，通过 VPC 实现不同业务系统隔离，VPC 内使用安全组隔离 VPC 内子网。各专业接口服务器需互相访问时通过 VPC 关联外部网络绕行实现，利用虚拟防火墙实现各 VPC 间精确网络互通控制。



为满足各业务系统之间的隔离与互访需求，需梳理各业务系统内对外通信服务器使用的 IP 地址、端口、对端设备 IP 地址、对端设备端口及通信协议。通过与 VPC 相关联的虚拟防火墙上进行策略（单向、双向）放通与阻断，实现业务系统间、云平台内与云平台外的网络访问控制。

业务系统互访关系：

业务系统	接口设备	对端业务系统	对端接口设备
综合监控	中心 FEP3	ATS	通信前置机 1
综合监控	中心 FEP3	CCTV	服务器
综合监控	中心 FEP3	PIS	接口服务器
综合监控	中心 FEP3	MLC	前置机
综合监控	中心 FEP3	CAS	集中告警服务器
综合监控	中心 FEP3	EMS	能源管理服务器
综合监控	中心 FEP4	ATS	通信前置机 2
综合监控	中心 FEP4	CCTV	服务器
综合监控	中心 FEP4	PIS	接口服务器
综合监控	中心 FEP4	MLC	前置机
综合监控	中心 FEP4	CAS	集中告警服务器
综合监控	中心 FEP4	EMS	能源管理服务器
综合监控	各车站云桌面	ACS	负载均衡
集中告警	集中告警服务器	PBE	工作站
集中告警	集中告警服务器	PIS	接口服务器
集中告警	集中告警服务器	时钟系统	时钟源
集中告警	集中告警服务器	广播 PA	
集中告警	集中告警服务器	专用电话	
集中告警	集中告警服务器	1 号线时钟	
集中告警	集中告警服务器	集中录音	
集中告警	集中告警服务器	CCTV	

信号 ATS 系统	通信前置机 1	PIS	接口服务器
信号 ATS 系统	通信前置机 1	ISCS	中心 FEP3
信号 ATS 系统	通信前置机 1	广播系统	
信号 ATS 系统	通信前置机 1	集群调度	
信号 ATS 系统	通信前置机 1	时钟系统	时钟源
信号 ATS 系统	通信前置机 1	数据共享	nginx
信号 ATS 系统	通信前置机 2	PIS	接口服务器
信号 ATS 系统	通信前置机 2	ISCS	中心 FEP4
信号 ATS 系统	通信前置机 2	广播系统	
信号 ATS 系统	通信前置机 2	集群调度	
信号 ATS 系统	通信前置机 2	时钟系统	时钟源
信号 ATS 系统	通信前置机 2	数据共享	nginx

防火墙规则实例：

序号	状态	动作	协议	源地址	端口	目的地址	端口	描述
1	启用	允许	TCP	10.103.19.10/32	8080	172.16.1.67/32	8080	AAA 接口设备-BBB 接口设备
2	启用	允许	TCP	172.16.1.67/32	8080	10.103.19.10/32	8080	BBB 接口设备-AAA 接口设备

对于业务系统内部网络控制主要通过安全组实现，安全组可视为一组特定的安全策略，与虚拟机的网卡关联，默认规则为阻断外部向内访问虚拟机，虚拟机向外访问不受限制。因此，设置安全组规则时只需添加源地址即可。城轨业务中主要用于信号系统 ATS 网络、综合监控网络的冗余网络（AB 网）间隔离。设置规则时，安全组添加规则应包含需放通通信的所有网段，如信号 ATS 系统的 A 网安全组，则应包含全部 A 网网段。

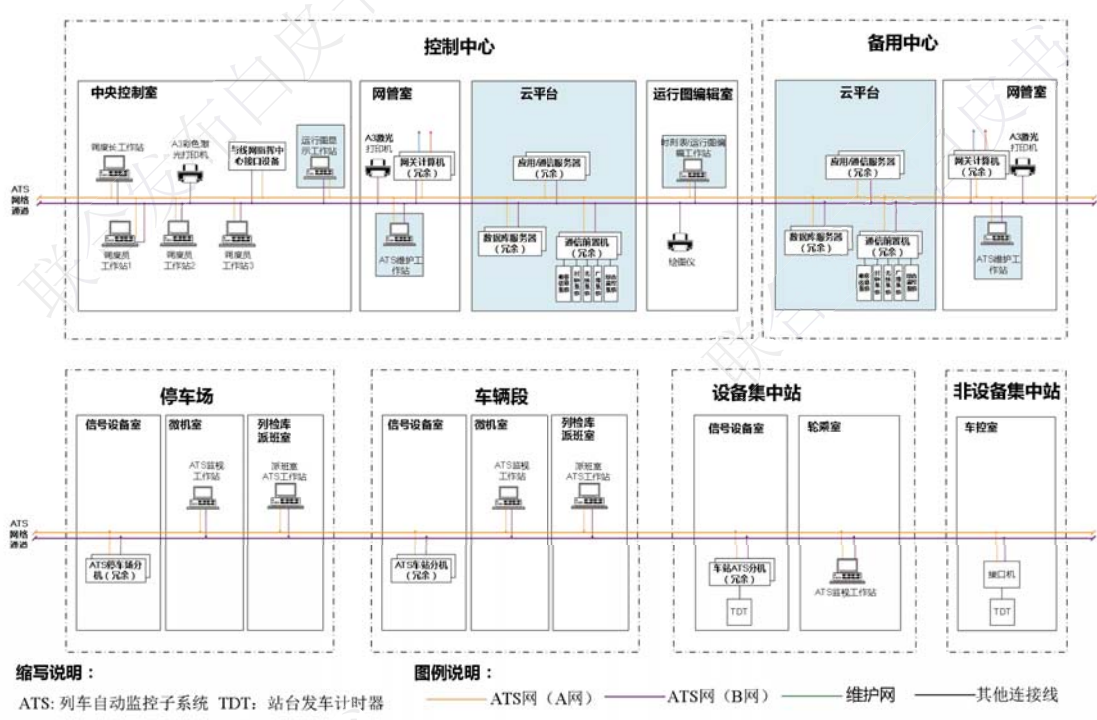
3.7.6. 典型业务系统部署实例

3.7.6.1.ATS

列车自动监控系统（ATS）是城市轨道交通信号系统的重要组成，ATS 通过对列车运行监视、自动排列进路、自动列车调整、自动生成时刻表、自动记录和统计运行数据并生成报表、自动检测设备运行状态等实现对列车运行的监视和控制，辅助调度员对全线列车进行管理。考虑 ATS 系统是 SIL2 级安全系统以及 ATS 系统数据流封闭性，建议 ATS 系统采用 IaaS

部署。同时，考虑云平台可能发生故障，出于安全考虑，建议车站 ATS 设备使用物理服务器形式，满足降级模式使用。

典型 ATS 系统在主用中心主要设置应用服务器、数据库服务器、通信前置机、运行图编辑工作站、时刻表编辑工作站、调度工作站、ATS 维护工作站等设备，ATS 云平台部署时，主要对中心设备进行云化迁移，可将应用服务器、数据库服务器、通信前置机、时刻表编辑工作站、运行图显示工作站、ATS 维护工作站（可选）云化部署，详见上云架构图。未来可逐步尝试扩大上云范围。



ATS 系统作为信号系统的“大脑”，应用自身需具备异地容灾能力和“中心-车站”两级控制能力。云平台作为线网级统一平台，设置主用中心和灾备中心，双中心通过 OTN 设备实现互联互通，通过信号自组网实现同时接入车站信号网络。云平台为信号系统创建独立的 VDC，保障其资源隔离性，同时利用 VPC 区分不同线路，实现同一入口对不同物理环境统一管控。

1、 区域划分

信号 ATS 子系统在主备双中心的安全生产网均有资源，分属于两个 Region：AQSC1、AQSC2。其中，数据库服务器属于裸金属可用区域（BMS_AZ），应用服务器、通信前置机属于云服务器可用区域（KVM_AZ）。

2、 子网划分

信号 ATS 子系统的虚拟私有云 AQSC1_ATS_Line1_VPC 包含：

AQSC1_ATS_Line1_SUB_A 网：用于 ATS 系统应用服务器、数据库服务器紫网；

AQSC1_ATS_Line1_SUB_B 网：用于 ATS 系统应用服务器、数据库服务器黄网；

AQSC1_ATS_Line1_SUB_FEP_A 网：用于 ATS 系统通信前置机紫网；

AQSC1_ATS_Line1_SUB_FEP_B 网：用于 ATS 系统通信前置机黄网；

VPC 内部子网：

AQSC1_ATS_Line1_INN_内部子网_A 网：用于紫网心跳的内部子网，仅 VPC 内部通信；

AQSC1_ATS_Line1_INN_内部子网_B 网：用于黄网心跳的内部子网，仅 VPC 内部通信。

3、资源需求

ATS 系统数据库服务器安装 Oracle 数据库，要求硬件独立，同时基于性能、稳定性、安全性考虑建议采用裸金属服务器承载。应用服务器、通信前置机无特殊限制建议采用虚拟机承载，具体资源需求如下：

服务器	CPU	内存	磁盘/G	共享盘/G	类型
数据库服务器 1	32	192	2*1200	3072	裸金属
数据库服务器 2	32	192	2*1200		裸金属
应用服务器 1	16	32	1000	/	云服务器
应用服务器 2	16	32	1000	/	云服务器
互联互通前置机	16	32	1000	/	云服务器
互联互通前置机	16	32	1000	/	云服务器
通信前置机 1	16	32	1000	/	云服务器
通信前置机 2	16	32	1000	/	云服务器
时刻表编辑工作站	8	16	2000	/	云桌面
运行图显示工作站	8	16	2000	/	云桌面

3.7.6.2.ISCS

综合监控系统（ISCS）通过对电力设备、火灾报警、信息及其设备、车站环控设备、区间环控设备、环境参数、屏蔽门设备、防淹门设备、电扶梯设备、照明设备、门禁设备、自动售检票设备、广播和闭路电视设备、乘客信息显示系统的播出信息和时钟信息等进行实时集中监视和控制。

ISCS 系统作为实现多专业联动的重要平台，其应用本身具备“中心-车站”两级控制能力，其系统也是由中心系统、车站级系统两级构成。云平台作为线网级统一平台，设置主用中心

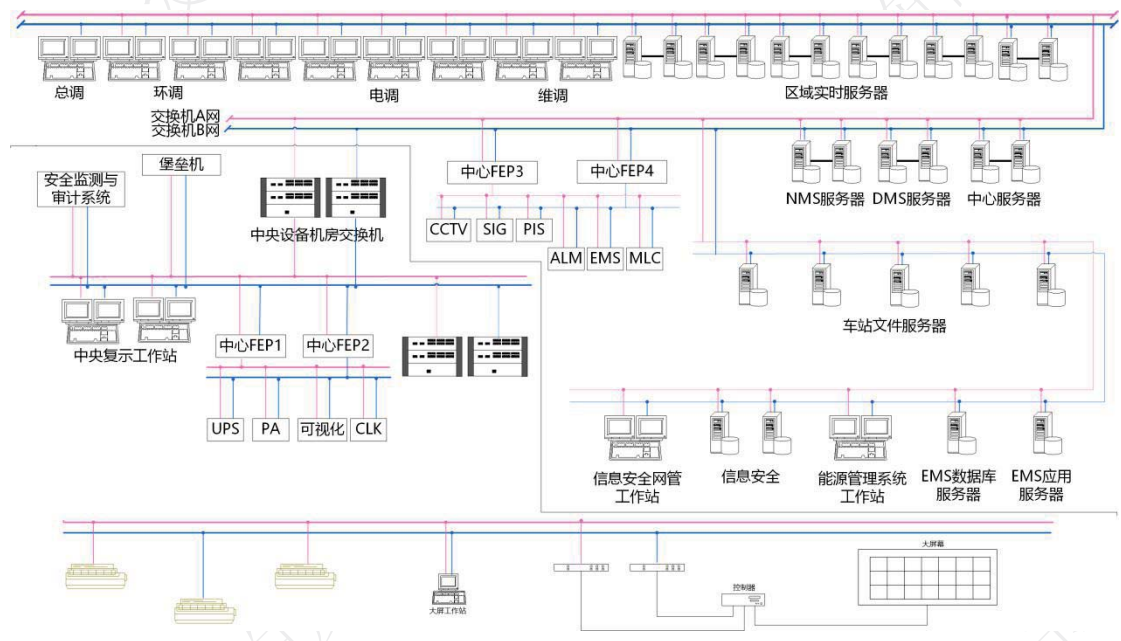
和灾备中心，呼和浩特云平台的灾备中心实现了综合监控系统数据灾备的能力。如果灾备中心增加适当的计算资源，综合监控业务应可实现应用级灾备。

综合监控在呼和浩特云平台落地方案如下面两张图所示。

中心系统，绝大部分都部署到云平台上：

上云的组件包括：区域实时服务器、网管系统（NMS）、维护管理系统（DMS）、车站文件服务器、中心 FEP（图中的中心 FEP3、FEP4）、调度终端（如电调、环调、维调，部署在云桌面上）。除了综合监控系统的主要组件外，还有一些辅助支持系统部署在云上，如信息安全系统、EMS（能源管理）系统等。

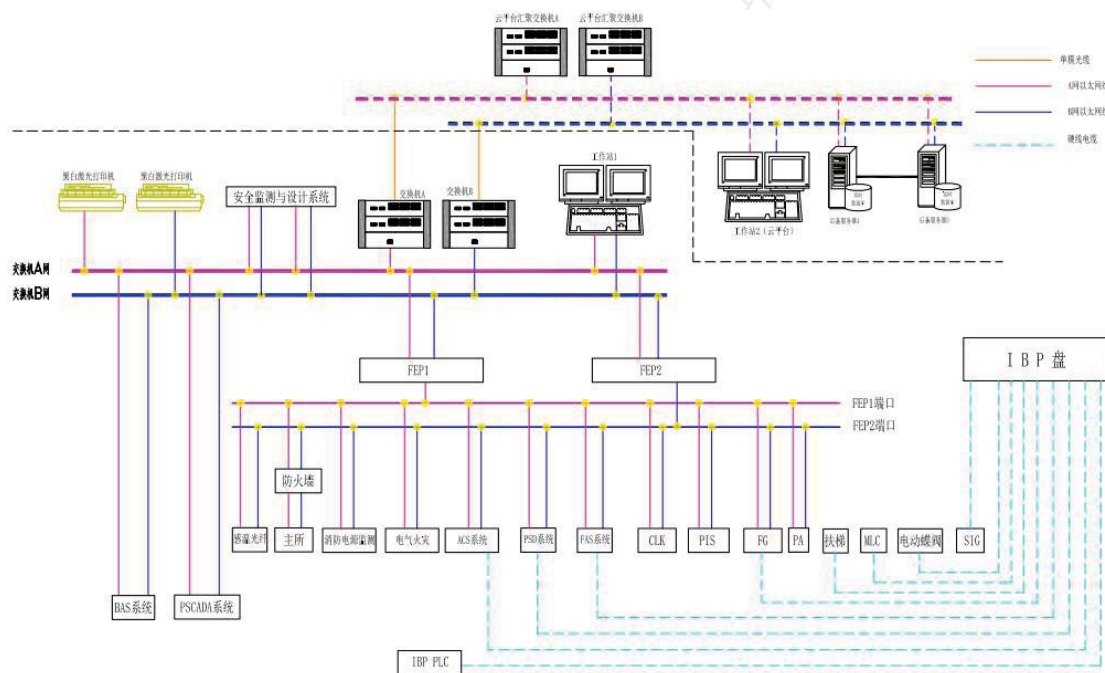
云下组件：中心 FEP（图中的中心 FEP1、FEP2）、大屏系统、安全系统（安全监控与审计、堡垒机等）及部分工作站。中心云下 FEP 按需串口相连的系统，如 UPS、广播等。



车站系统，仍保持大量云下互联部分：

站段云上部署综合监控后备服务器，以及 1 台云桌面工作站。

综合监控系统在站段云下部署了 FEP、物理工作站、安全检测与设计系统。云下 FEP 对接了 BAS、FAS、PSCADA、时钟、广播、屏蔽门等系统。采集了这些站级系统信息之后，通过综合监控系统云下交换机接至站段云，再通过站段云汇聚交换机和云平台专用传输通道传至中心。



主用中心云平台的设置：

1) 区域划分

ISCS 系统在主要在主用中心的安全生产网有计算资源，属于一个 Region: AQSC1；其中，数据库服务器属于裸金属可用区域（BMS_AZ），区域实时服务器、通信前置机属于云服务器可用区域（KVM_AZ）。

2) 子网划分

ISCS 系统的虚拟私有云 AQSC1_ISCS_Line1_VPC 包含：

AQSC1_ISCS_Line1_SUB_A 网：用于 ISCS 系统区域实时服务器、数据库服务器 A 网；

AQSC1_ISCS_Line1_SUB_B 网：用于 ISCS 系统区域实时服务器、数据库服务器 B 网；

AQSC1_ISCS_Line1_SUB_FEP_A 网：用于 ISCS 系统通信前置机 A 网；

AQSC1_ISCS_Line1_SUB_FEP_B 网：用于 ISCS 系统通信前置机 B 网；

AQSC1_ISCS_Line1_SUB_NMS_A 网：用于 ISCS 系统 NMS A 网；

AQSC1_ISCS_Line1_SUB_NMS_B 网：用于 ISCS 系统 NMS B 网；

AQSC1_ISCS_Line1_SUB_DMS_A 网：用于 ISCS 系统 DMS A 网；

AQSC1_ISCS_Line1_SUB_DMS_B 网：用于 ISCS 系统 DMS B 网；

3) 资源需求

ISCS 系统数据库服务器安装 MySQL 数据库，要求硬件独立，同时基于性能、稳定性、

安全性考虑建议采用裸金属服务器承载。应用服务器、通信前置机无特殊限制建议采用虚拟机承载，具体资源需求如下：

服务器	CPU	内存	磁盘	共享盘	类型
区域实时服务器 1-1	16	64	600	/	云服务器
区域实时服务器 1-2	16	64	600	/	云服务器
区域实时服务器 2-1	16	64	600	/	云服务器
区域实时服务器 2-2	16	64	600	/	云服务器
区域实时服务器 3-1	16	64	600	/	云服务器
区域实时服务器 3-2	16	64	600	/	云服务器
区域实时服务器 4-1	16	64	600	/	云服务器
区域实时服务器 4-2	16	64	600	/	云服务器
区域实时服务器 5-1	16	64	600	/	云服务器
区域实时服务器 5-2	16	64	600	/	云服务器
区域实时服务器 6-1	16	64	600	/	云服务器
区域实时服务器 6-2	16	64	600	/	云服务器
区域实时服务器 7-1	16	64	600	/	云服务器
区域实时服务器 7-2	16	64	600	/	云服务器
中心历史服务器 1	32	192	2400	2500	裸金属
中心历史服务器 2	32	192	2400		裸金属
DMS 服务器 1	32	192	2400	2500	裸金属
DMS 服务器 2	32	192	2400		裸金属
通信前置机 3	4	4	40		云服务器
通信前置机 4	4	4	40		云服务器
数据分析服务器	16	64	600	/	云服务器
软件测试平台服务器	16	64	600	/	云服务器
终端安全管理系统	16	16	500	/	云服务器

工控安全管理平台	16	32	3000	/	云服务器
监控审计管理平台	16	32	2400	/	云服务器
总调工作站	8	16	300		云桌面
环调工作站 1	8	16	300		云桌面
环调工作站 2	8	16	300		云桌面
电调工作站 1	8	16	300		云桌面
电调工作站 2	8	16	300		云桌面
行调工作站 1	8	16	300		云桌面
行调工作站 2	8	16	300		云桌面
维调工作站	8	16	300		云桌面
车站工作站	8	16	300		各站云桌面
车站 ISCS	8	16	500		各站服务器

3.7.6.3.AFC

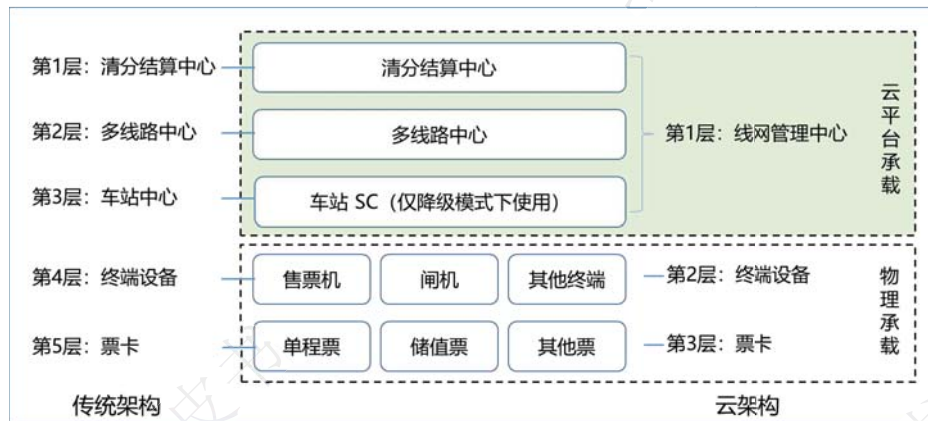
AFC 系统是基于计算机、通信、网络、自动控制等技术，能够实现轨道交通售票、检票、计费、收费、统计、清分、管理自动化进行。AFC 系统是地铁乘客使用频率最高的专业系统，其设备与系统制造、集成、调试及维护质量，关系到地铁运营安全。AFC 系统以云平台为基础环境，整合计算资源、存储资源、网络资源、安全资源，依托于云平台灵活的资源管理，实现对 ACC 系统、MLC 系统、SC 系统（后备模式下）、互联网票务平台系统进行灵活的部署，最大程度利用数据中心资源，降低硬件成本。

云平台环境下将传统的五层 AFC 系统架构精简至三层 AFC 系统架构。

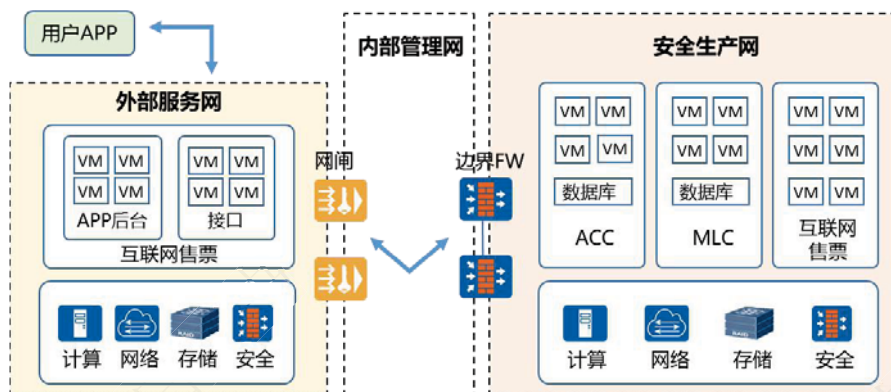
第一层：线网管理中心，主要包括 ACC 系统、MLC 系统、SC 系统（降级模式下）、互联网票务平台、一卡通以及第三方支付接口。

第二层：车站终端设备，包括闸机、自动售票机、自动检票机、互联网终端等。

第三层：读写器、二维码读头，可以对非接触式票卡、二维码等多种票务凭据进行处理。



对于云平台承载的部分，按照其信息交互及服务对象不同，又分属于安全生产网及外部服务网。安全生产网主要承载清分结算中心系统、多线路中心系统和车站中心系统，其中加密认证机、密钥管理、编码分拣等使用物理设备部署。外部服务网承载互联网售票的 APP 后台系统、接口系统。AFC 业务部署于安全生产网和外部服务网的应用，属于不同安全域，不能直接访问，需借助内部管理网通道实现业务互访。其中，安全生产网和内部管理网之间通过边界防火墙仅放通需要经过的 IP、端口、协议，内部管理网和外部服务网之间通过网闸完成数据摆渡。



主用中心云平台的设置:

1) 区域划分

AFC 系统在安全生产网的计算资源属于一个 Region: AQSC1。其中，数据库服务器属于裸金属可用区域 (BMS_AZ)，应用服务器、接口服务器等属于云服务器可用区域 (KVM_AZ)。

2) 子网划分

- ACC 系统的虚拟私有云 AQSC1_AFC_ACC_VPC 包含:

AQSC1_AFC_ACC_SUB: 用于 ACC 系统消息队列、交易系统、对账、清分等;

AQSC1_AFC_ACC_SUB_互联网: 用于 ACC 互联网售票系统第三方支付、发码平台、二

维码验证平台等；

AQSC1_AFC_ACC_SUB_票务：用于票务系统的注册中心、配置中心、夜结服务、前端服务等；

- MLC 系统的虚拟私有云 AQSC1_AFC_MLC_VPC 包含：

AQSC1_AFC_MLC_SUB：用于 MLC 系统的消息队列、接入系统、边缘计算等；

3) 外服网子网划分

WBFW_AFC_4：用于外部服务网中 AFC 互联网售票子系统。

4) 资源需求

AFC 系统数据库服务器安装 Oracle RAC 数据库，要求硬件独立，同时基于性能、稳定性、安全性考虑建议采用裸金属服务器承载。应用服务器、接口服务器等无特殊限制的采用虚拟机承载，具体资源需求如下：

服务器	CPU	内存	磁盘	共享盘	类型
消息队列 1	32	32	300		云服务器
消息队列 2	32	32	300		云服务器
内存数据库 1	8	8	200		云服务器
内存数据库 2	8	8	200		云服务器
数据库 1	\	\	\	17600	裸金属
数据库 2	\	\	\		裸金属
接入子系统 1	8	16	300		云服务器
接入子系统 2	8	16	300		云服务器
交易-业务-事件-客流 1	8	16	500		云服务器
交易-业务-事件-客流 2	8	16	500		云服务器
参数-模式-用户-日志-ACC 系统管理	8	8	300		云服务器
审计-对账-清分 1	8	32	300		云服务器
审计-对账-清分 2	8	32	300		云服务器
数据服务子系统	8	16	500		云服务器
网络管理子系统	4	4	200		云服务器

ES 管理子系统	4	4	200		云服务器
密钥管理子系统	4	8	200		云服务器
密钥认证子系统 1	8	8	200		云服务器
密钥认证子系统 2	8	8	200		云服务器
iTVM-对账及审计 1	6	16	300		云服务器
iTVM-对账及审计 2	6	16	300		云服务器
第三方支付 1	6	16	300		云服务器
第三方支付 2	6	16	300		云服务器
发码平台 1	6	16	300		云服务器
发码平台 2	6	16	300		云服务器
发码平台 3	6	16	300		云服务器
密钥服务 1	6	16	300		云服务器
密钥服务 2	6	16	300		云服务器
Iag-二维码验码平台 1	6	16	300		云服务器
iAG-二维码验码平台 2	6	16	300		云服务器
iAG-二维码验码平台 3	6	16	300		云服务器
iAG-二维码验码平台 4	6	16	300		云服务器
基础信息 1	8	32	300		云服务器
基础信息 2	8	32	300		云服务器
基础信息 3	8	32	300		云服务器
基础信息 4	8	32	300		云服务器
管理服务 1	6	16	300		云服务器
管理服务 2	6	16	300		云服务器
线路前置 1	8	32	300		云服务器
线路前置 2	8	32	300		云服务器
互联网 1	6	16	300		云服务器

互联网 2	6	16	300		云服务器
互联网 3	6	16	300		云服务器
互联网 4	6	16	300		云服务器
互联网 5	6	16	300		云服务器
互联网 6	6	16	300		云服务器
ACC-注册中心 1	8	8	300		云服务器
ACC-注册中心 2	8	8	300		云服务器
ACC-注册中心 3	8	8	300		云服务器
ACC-配置中心 1	4	8	300		云服务器
ACC-配置中心 2	4	8	300		云服务器
ACC-基础服务-系统管理服务 1	4	8	300		云服务器
ACC-基础服务-系统管理服务 2	4	8	300		云服务器
ACC-车票管理服务-现金管理服务 1	4	8	300		云服务器
ACC-车票管理服务-现金管理服务 2	4	8	300		云服务器
ACC-夜结服务-前端服务 1	4	8	500		云服务器
ACC-夜结服务-前端服务 2	4	8	500		云服务器
ACC-夜结服务-前端服务 3	4	8	500		云服务器
ACC-消息处理服务 1	8	8	300		云服务器
ACC-消息处理服务 2	8	8	300		云服务器
ACC-消息处理服务 3	8	8	300		云服务器
ACC-网关服务 1	4	8	300		云服务器
ACC-网关服务 2	4	8	300		云服务器
ACC-网关服务 3	4	8	300		云服务器
ACC-报表服务	8	8	300		云服务器
ACC-日志服务	8	16	500		云服务器
MLC-管理中心-配置中心 1	4	16	300		云服务器

MLC-管理中心-配置中心 2	4	16	300		云服务器
MLC-管理中心-配置中心 3	4	16	300		云服务器
MLC-基础服务-系统管理 1	4	8	300		云服务器
MLC-基础服务-系统管理 2	4	8	300		云服务器
MLC-车票管理-现金管理服务	4	8	300		云服务器
MLC-BOM 管理服务-TVM 管理服务	4	8	300		云服务器
MLC-夜结服务 1	8	16	500		云服务器
MLC-夜结服务 2	8	16	500		云服务器
MLC-夜结服务 3	8	16	500		云服务器
MLC-报表服务	8	16	300		云服务器
MLC-消息处理服务 1	8	16	300		云服务器
MLC-消息处理服务 2	8	16	300		云服务器
MLC-消息处理服务 3	8	16	300		云服务器
MLC-前端服务-网关服务 1	8	8	300		云服务器
MLC-前端服务-网关服务 2	8	8	300		云服务器
MLC-前端服务-网关服务 3	8	8	300		云服务器
MLC-日志服务	8	16	500		云服务器
消息队列 1	32	64	300		云服务器
消息队列 2	32	64	300		云服务器
内存数据库 1	8	8	300		云服务器
内存数据库 2	8	8	300		云服务器
数据库 1	\	\	\	6600	裸金属
数据库 2	\	\	\		裸金属
接入系统 1	8	16	300		云服务器
接入系统 2	8	16	300		云服务器
接入系统 3	8	16	300		云服务器

接入系统 4	8	16	300		云服务器
接入系统 5	8	16	300		云服务器
接入系统 6	8	16	300		云服务器
ACC 接入系统	8	16	500		云服务器
交易-业务-事件-客流管理子系统 1	8	32	500		云服务器
交易-业务-事件-客流管理子系统 2	8	32	500		云服务器
设备监视-运行控制-设备维修-ISCS1	8	16	300		云服务器
设备监视-运行控制-设备维修-ISCS2	8	16	300		云服务器
参数-用户-车站-日志-MLC 管理	8	16	300		云服务器
数据审计-清分对账	8	16	300		云服务器
数据服务子系统	8	16	200		云服务器
网络管理子系统	4	8	200		云服务器
接入系统 1	8	16	300		云服务器
接入系统 2	8	16	300		云服务器
接入系统 3	8	16	300		云服务器
接入系统 4	8	16	300		云服务器
接入系统 5	8	16	300		云服务器
接入系统 6	8	16	300		云服务器
边缘计算 1	4	16	300		云服务器
边缘计算 2	4	16	300		云服务器
边缘计算 3	4	16	300		云服务器
边缘计算 4	4	16	300		云服务器
边缘计算 1	4	16	300		云服务器
边缘计算 2	4	16	300		云服务器
边缘计算 3	4	16	300		云服务器
边缘计算 4	4	16	300		云服务器

边缘计算 5	4	16	300		云服务器
边缘计算 6	4	16	300		云服务器
监控服务器	8	16	300		云服务器
外服网-APP 后台 1	8	64	1024		云服务器
外服网-APP 后台 2	8	64	1024		云服务器
外服网-APP 外部接口 1	8	64	1024		云服务器
外服网-APP 外部接口 2	8	64	1024		云服务器
外服网-APP 服务 1	8	64	1024		云服务器
外服网-APP 服务 2	8	64	1024		云服务器
中心工作站 x17	4	6	200		云桌面
车站云桌面	8	8	200		各站云桌面
各车站降级服务器	8	8	200		降级资源
各车站降级桌面	8	8	200		降级资源

4. 大数据平台

大数据平台建设旨在通过收集分散在各设备、各系统内大量有价值的数据，通过分析、挖掘、展现，以达到用数据指导运营、运维工作的目的，充分发挥数据价值，以数据提供服务。在城市轨道交通行业，还没有可供参考的大大数据平台建设应用范例。但可以预见到的是，无论在何种领域，大数据平台建设应用的目标绝不是一成不变的，它应在平台所承载的应用不断扩展的同时，具备持续为用户提供直观准确快速有效的数据信息，以支持运营管理决策；持续对设备亚健康状态进行监测，提升设备管理效率，减少人工成本。

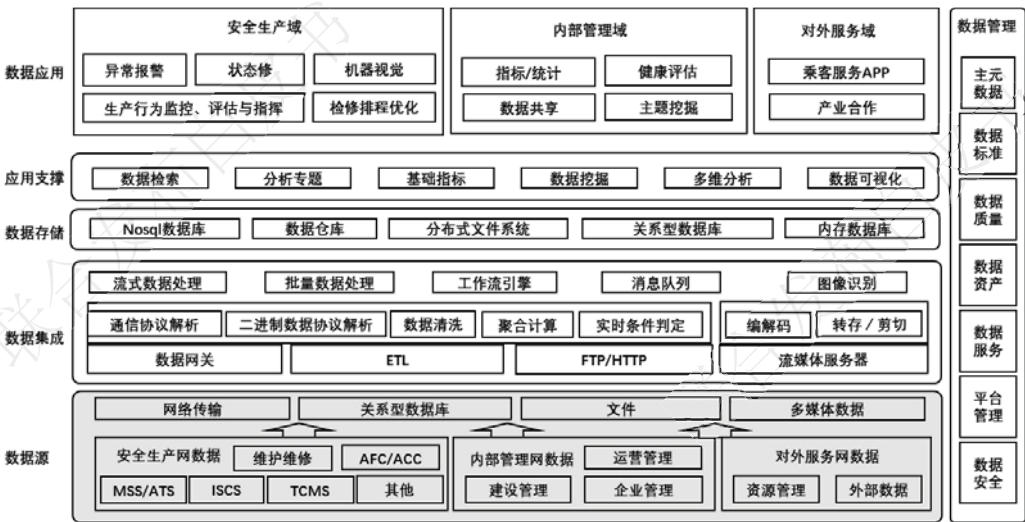
基于以上目标，大数据平台需做到对于不同类型、不同专业的海量数据采用不同的采集和存储策略，确保平台的稳定性和安全性，同时还应保证上层应用在做数据提取时的效率和准确性，最后再依据业务要求构建不同类型的数据应用。

企业数字化的建设和转型，不只是管理创新、大数据的建设和应用，同时还需要长期的对大数据团队的投入。拥有了解业务和相关技术的核心团队成员，才能真正把大数据平台用好，为企业创造更大的价值，更好的为业务和管理服务。

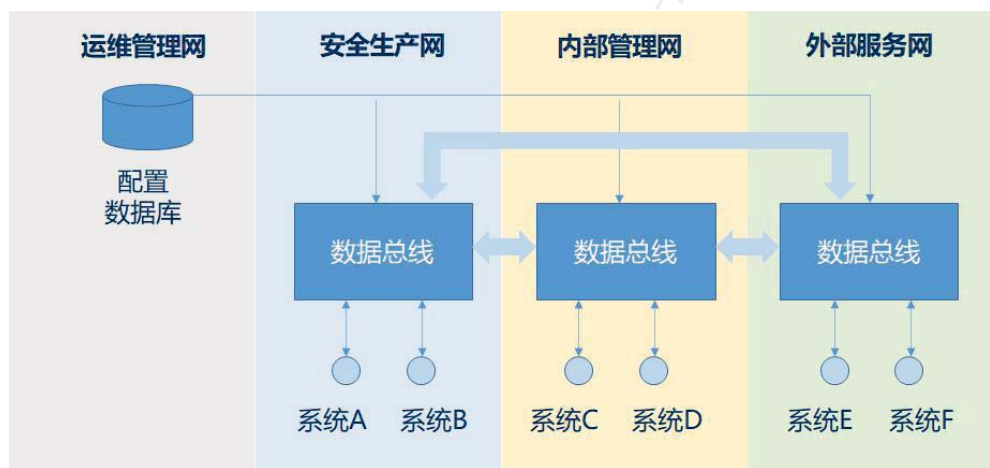
4.1. 大数据平台总体架构

大数据平台用于承载安全生产网各业务系统产生的生产数据，数据经过平台的处理后，为上层数据的应用和展示提供支撑。

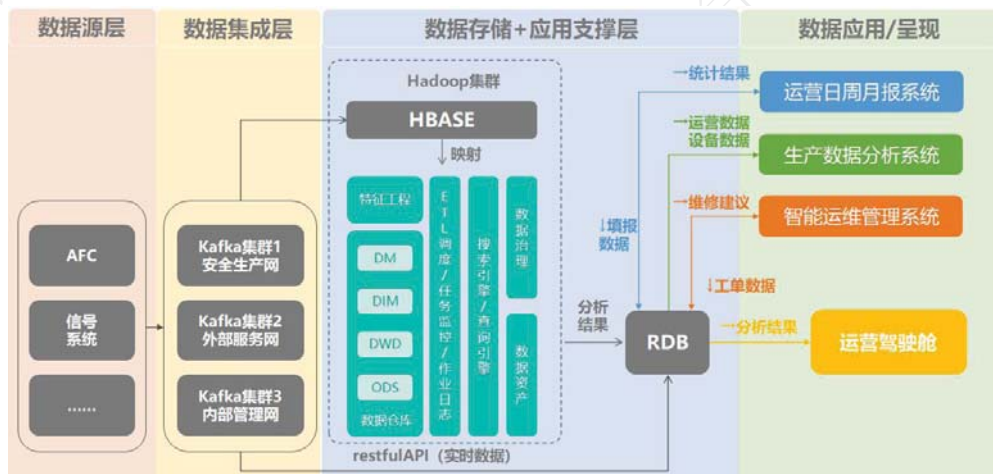
协会《规范》中对大数据平台的逻辑架构图见下：



《规范》中大数据平台共分为 5 层：数据源层、数据集成层、数据存储层、应用支撑层和数据应用层，还有一个数据管理功能贯穿全平台。从部署架构上来看，安全生产网、内部网、外部服务网均可部署大数据平台，在运维管理网中部署平台级的管理系统。各网域间数据互通是通过数据总线相连实现，跨网域的数据传输须经过边界安全设备。



呼和浩特城轨云落地实现上，通过简化相关的配置，将应用支撑层功能与数据存储层合并，由一套组件实现其功能。仅在安全生产网中部署了大数据平台，没有跨网域的数据流量，也没有全平台的管理系统。呼和浩特城轨云大数据平台架构如下：



呼和浩特城轨云大数据平台主要分为 2 层：数据集成层、数据存储+应用支撑层。数据集成层实现了消息队列和流式数据处理功能。数据存储+应用支撑层实现了数据仓库、分布式文件系统、关系型数据库、分析专题、数据可视化等功能。

源数据通过 kafka 集群以流的方式传递进入大数据平台，数据会首先存入 Hadoop 集群 hbase 数据库。为便于后续计算及处理，大数据平台会对原始数据进行数据清洗，对数据类型和差错数据进行处理之后，形成贴源数据存储于数据仓库（Hive）当中。数据仓库会根据数据应用的使用需求，分成不同的数据主题，对这些贴源数据再次进行计算和存储。最终的统计和分析结果会同步存储在关系型数据库（RDB）中，各个数据应用从关系型数据库中获取结果数据，而数据应用产生的数据也会回写入 RDB 中以供后续分析。

对于数据实时性要求较高的系统，RDB 具备通过标准 restfulAPI 接口直接与数据共享平台通信，获取实时数据的能力。

数据仓库的数据来源于不同的源数据，并提供多样的数据应用，数据自下而上流入数据

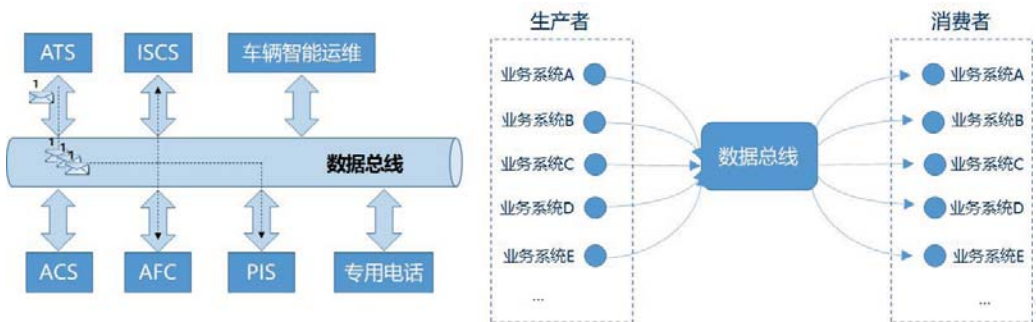
仓库后向上层开放应用。作为中间集成化数据管理的平台，为了保证大数据平台的整体用户体验，数据仓库对数据由下而上进行了分层管理。

呼和浩特城轨云大数据平台在建设期包含 2 类、4 种数据应用：1、运营管理类业务，包含运营日周月报系统、运营驾驶舱 2 个应用。2、设备监测及运维类业务，主要是智能运维管理系统。还有一个生产数据分析系统属于数据综合应用，既包含运营管理类数据，又包含设备类数据。

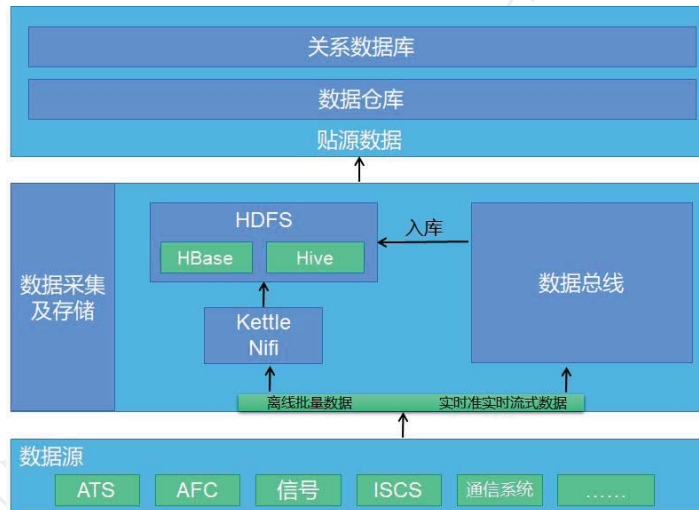
4.2. 数据集成层

呼和浩特城轨云大数据平台的数据集成层主要实现了数据总线功能，包括用户权限管理、数据生产者管理、数据消费者管理、数据持久化等。

- 1) 用户权限管理：基于通用的 RBAC 的方式进行管理。
- 2) 数据生产者管理：是对数据生产者的配置管理。
- 3) 数据消费者管理：是消费者选择所需数据的管理。
- 4) 数据持久化：各专业系统通过数据集成层传输的业务数据，平台会对数据做持久化处理，为后续数据挖掘提供支持。



底层使用 Kafka 消息队列系统实现了数据总线功能，实现了对业务系统 Restful 的接口，用于实时准实时流式数据的传输。除了流式数据外，平台还支持以接口文件形式传输离线批量数据。数据采集总体流程如下：



离线批量数据：根据需求划分数据源，根据事实表和维度表，分别做增量和全量的采集。采用接口文件进行数据推送。离线数据的抽取分为两大部分：一部分是直接从源业务系统中进行数据抽取，该部分数据不包含已经实时同步到数据共享平台的数据内容；一部分是从数据共享平台中做数据 T+1 的抽取。

实时/准实时流式数据：采用 Flume+Kafka+Hbase 的开源组件，构建实时日志数据的采集框架。一方面在数据平台上做数据的存储，另一方面通过共享数据平台与其他业务系统进行实时交互。

数据管理层为需要接入平台的各业务系统提供实时数据交互和历史数据获取的功能。平台支持网内各业务系统的数据交互共享。数据管理层向业务系统提供历史数据时，只支持从平台所维护的数据库抽取历史数据。

协会《规范》中网域间的数据可实现互通。

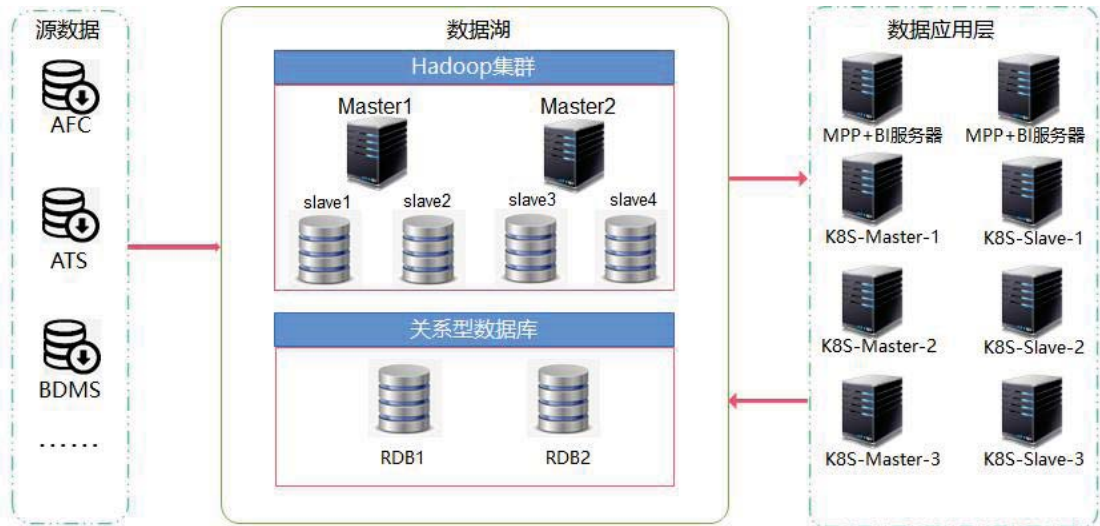
为实现实时业务数据的“一次发布，多方消费”，数据总线采用基于主题的发布订阅机制实现。作为数据生产者的业务系统将业务数据发布给数据总线，而不是直接发送给特定业务系统。作为数据消费者的业务系统，需要提前订阅相关数据主题。当平台上该主题数据更新时，消费者业务系统将自动实时获取所订阅的数据。

数据管理层应具备良好的易用性。各业务系统可采用“热插拔”方式接入。当业务系统接入平台时，平台能够自动发现该业务系统，并提供数据发布订阅服务。当业务系统断开时，不会影响平台的正常运行。当新增需向平台发布的主题数据时，只需修改配置参数，平台无需重新启动，即可提供新增主题数据的发布订阅服务。

数据管理层应具备业务系统访问权限管理功能。只有平台授权的业务系统，才可能使用平台的发布订阅服务。只有在平台注册的主题数据，才能发布供其它业务系统订阅使用。平台管理员可以指定业务系统可订阅的主题范围，在业务系统订阅平台主题数据时，所订阅主题不能超过该范围。平台具备主题管理（增删改查）功能。

4.3. 数据存储+应用支撑层

呼和浩特城轨云大数据平台的数据存储+应用支撑层集成了 Hadoop 集群和关系型数据库，Hadoop 集群用于存储各业务系统的原始数据及非结构化数据，关系型数据库（RDB）用于存储整理后的结构化数据。数据应用由 2 部分构成：K8S 管理的容器系统，用于承载数据应用系统；MPP+BI，用于驾驶舱及数据展示相关内容。



安装的功能组件：

- 1) Hadoop-Master1: Hadoop、Scala、Spark、Hbase
- 2) Hadoop-Master2: Hadoop、Scala、Spark、Hbase
- 3) Hadoop-Slave1: Hadoop、Zookeeper、Scala、Spark、Kafka、Hbase
- 4) Hadoop-Slave2: Hadoop、Zookeeper、Scala、Spark、Kafka、Hbase
- 5) Hadoop-Slave3: Hadoop、Zookeeper、Scala、Spark、Kafka、Hbase
- 6) Hadoop-Slave4: Hadoop、Hive、Oozie、Sqoop、Nifi、Flume、Scala、Spark、Hbase
- 7) 关系型数据库: Postgresql

相关配置如下：

序号	CPU / vCPU	内存 / GB	存储 / TB	部署形式	用途
1	64	128	10	物理机	Name-Node-1
2	64	128	10	物理机	Name-Node-2
3	64	128	35	物理机	Data-Node-1
4	64	128	35	物理机	Data-Node-2

5	64	128	35	物理机	Data-Node-3
6	64	128	35	物理机	Data-Node-4
7	16	10	0.5	虚拟机	K8S-Master-1
8	16	10	0.5	虚拟机	K8S-Master-2
9	16	10	0.5	虚拟机	K8S-Master-3
10	8	8	0.5	虚拟机	K8S-Slave-1
11	8	8	0.5	虚拟机	K8S-Slave-2
12	8	8	0.5	虚拟机	K8S-Slave-3
13	8	8	1	虚拟机	关系型数据库-1
14	8	8	1	虚拟机	关系型数据库-2
15	8	16	1	虚拟机	MPP+BI
16	8	16	1	虚拟机	MPP+BI

Hadoop 系统的设计理念是将数据的存储和计算分布多台主机上，主机间使用高速网络相连。推荐使用万兆互联网口，本地存储，并采用裸金属纳管的形式接入云平台。

4.4. 数据应用

4.4.1. 运营管理类应用

运营管理功能的使用者偏向管理层，因此运营管理类的设计侧重于管理层需求，用以了解运营情况全貌，为决策提供支持。通过对运营数据的主题划分，用数据说话，从各个角度、向不同层级的管理人员呈现运营状态。其设计原则如下：

- 1、 根据用户层级不同进行设计，以不同用户层级日常的使用场景出发，分为总经理、副总、部门级，每个级别关注的的数据粒度和数据点不同；
- 2、 根据数据层级不同进行设计，既要满足实时数据展示的需要，也要满足各种维度的统计、对比分析（例如年月日、线路、站点等）。

基于行业的特殊性，将城市轨道交通运营中所产生的运营数据通过系统抽取和人工填报两种方式进行汇总，并通过运营信息驾驶舱和运营日周月报两种形式进行展示。汇集的数据主题包括客流信息主题、列车运行信息主题、电源消耗信息主题、安全主题、票卡主题、设备状态主题、维修情况主题数据。

运营信息驾驶舱根据上述主题，分成线网级、线路级、站点级、设备级四个层级。

运营日周月报的内容包括客运量情况、票卡情况、列车开行情况、列车使用情况、列车服务情况、运营里程、施工情况、电能消耗情况、其它情况共 9 项内容，对用户日常填写的数据和系统抽取的数据进行统计汇总，生成报表，各项内容的数据均进行日、周、月、年汇总，形成数据报表，支持在线查看和导出。系统通过对运营数据进行统筹管理，为决策提供必要的支持。

功能设计：

序号	功能模块	功能点	功能描述
1	数据管理	系统采集	客流情况（票卡）、列车开行情况、信号/AFC 设备故障状态数据采集
2		人工填报	运营里程、列车服务情况、电能消耗情况、施工情况、重大故障、其他情况数据填报
3		流程审批	查看、编辑、通过、驳回
4		数据查看	原始数据查看、导出
5		多条件筛选	填报人、数据采集时间、线路、站点等条件筛选
6	报告管理	最新报告查看	昨日、上周、上月报告
7		历史报告查阅	查看、导出
8	运营管理驾驶舱	总裁驾驶舱	全线网指标展示，支持下钻至各主题
9		运营管理驾驶舱	运营相关主题指标展示，支持下钻至各主题
10		设备管理驾驶舱	设备故障状态、设备维修状态指标展示，支持下钻至各主题
11		客流主题	实时数据查看；历史数据分析；多条件筛选
12		票卡主题	实时数据查看；历史数据分析；多条件筛选
13		行车主题	实时数据查看；历史数据分析；多条件筛选
14		列车服务主题	实时数据查看；历史数据分析；多条件筛选
15		电源消耗主题	实时数据查看；历史数据分析；多条件筛选
16		设备管理主题	实时数据查看；历史数据分析；多条件筛选
17		维修管理主题	实时数据查看；历史数据分析；多条件筛选
18		重大事件主题	实时数据查看；历史数据分析；多条件筛选
19	系统设置	用户管理	用户的增删改查

序号	功能模块	功能点	功能描述
20			用户密码管理
21			用户启用与禁用
22		权限管理	角色管理
26			人员管理
27		审批流管理	填报流程设置
28			流程角色设置
29		系统操作日志	查询

其中：

1) 数据管理

系统采集类的数据：下方会标注数据源，系统自动采集后，可设置相关人员进行查看、修改、确认和审批。

人工填报类数据：设置填报角色进行数据填报，并配置相关人员进行查看、修改、确认和审批。

2) 报告管理

报告生成后需要各层级上报、审批，才可最终呈现。生成的报告可随时查看。报告分为客运量情况、运营里程、列车开行情况、列车使用情况、列车服务情况、电能消耗情况、施工情况、重大故障、其他情况 9 个部分，汇集系统抽取的数据和人工填写的备注信息后，生成报告。

3) 运营管理驾驶舱

将收集到的数据根据不同层级的要求进行展示，展示终端分为大屏、PC 端两种，各显示终端展示重点各有侧重。大屏主要用于实时状态监测和外部参观，除保证数据的准确性、有效性，界面的设计应富有科技感。PC 端主要用于数据的分析，因此需要添加各种分析维度便于客户自行选择。

根据地铁运营公司组织架构，通常对界面进行如下设计：

从管理职能上来分析，运营公司董事长可查看到全线网的顶层指标，运营副总经理查看运营相关的顶层指标，设备副总经理或总工程师查看设备故障、维修情况的顶层指标，每个顶层指标可通过层层下钻至各主题的驾驶舱界面。

在设计各界面指标时，可参考 MOPES，结合用户实际需求进行设计。下方表格为参考：

序号	主题	指标名称
1	客流主题	当日进站量
2	客流主题	当日出站量
3	客流主题	当日实时客运量
4	客流主题	当日实时集散量
5	客流主题	昨日换乘客流量
6	客流主题	昨日高峰小时断面客流
7	客流主题	昨日拥挤度
8	客流主题	总客运量
9	客流主题	总进站
10	客流主题	上周进同比
11	客流主题	昨日进环比
12	客流主题	总出站
13	客流主题	上周出同比
14	客流主题	昨日出环比
15	客流主题	总进出站差值
16	客流主题	每日进站量趋势
17	客流主题	每月进站量趋势
18	客流主题	每日出站量趋势
19	客流主题	每月出站量趋势
20	客流主题	每日换乘量趋势
21	客流主题	每月换乘量趋势
22	客流主题	每日平均拥挤度趋势
23	客流主题	每月平均拥挤度趋势
24	行车主题	当日最小列车运行间隔

25	行车主题	昨日最小列车运行间隔
26	行车主题	历史最小列车运行间隔
27	行车主题	当日平均旅行速度
28	行车主题	昨日平均旅行速度
29	行车主题	历史平均旅行速度
30	行车主题	当日列车在各站实际到发时刻
31	行车主题	当日列车早晚点
32	行车主题	当日正点率
33	行车主题	昨日兑现率
34	行车主题	当日计划运行列车数
35	行车主题	昨日加开列车数
36	行车主题	昨日开行列数统计
37	行车主题	昨日掉线列数统计
38	行车主题	昨日请客列数统计
39	行车主题	上月列车服务可靠度统计
40	行车主题	本年截止到上月列车服务可靠度统计
41	行车主题	每日列车早晚点统计
42	行车主题	每月列车早晚点统计
43	行车主题	每日列车正点率
44	行车主题	每月列车正点率
45	行车主题	每日计划开行列次统计
46	行车主题	每月计划开行列次统计
47	行车主题	每日加开列次统计统计
48	行车主题	每月加开列次统计统计
49	行车主题	每月清客列数统计

50	行车主题	每月掉线列次统计
51	行车主题	每月司机驾驶公里数统计
52	行车主题	某个司机每月驾驶公里数统计
53	行车主题	延误运营事件数统计
54	行车主题	各月列车服务可靠度统计
55	票卡主题	昨日线网票卡收入总额
56	票卡主题	昨日各线路票卡收入总额
57	票卡主题	上周线网票卡收入同比
58	票卡主题	前日线网收入环比
59	票卡主题	当日票卡各类型分布
60	票卡主题	实时票卡数量
61	票卡主题	上周线网票卡数量同比
62	票卡主题	昨日线网票卡数量环比
63	票卡主题	每日票卡收入趋势
64	票卡主题	每月票卡收入趋势
65	票卡主题	每日票卡数量趋势
66	票卡主题	每月票卡数量趋势
67	电源消耗主题	网络能耗统计
68	电源消耗主题	网络牵引能耗
69	电源消耗主题	网络动力及照明能耗
70	电源消耗主题	网络每车公里牵引能耗
71	电源消耗主题	网络每人次牵引能耗
72	电源消耗主题	线路牵引能耗
73	电源消耗主题	线路动力及照明能耗
74	电源消耗主题	线路每车公里牵引能耗

75	电源消耗主题	线路每人牵引能耗
76	电源消耗主题	历史线网牵引能耗最大值
77	电源消耗主题	历史线网牵引能耗最小值
78	电源消耗主题	历史线网牵引能耗平均值
79	电源消耗主题	历史线网动力照明能耗最大值
80	电源消耗主题	历史线网动力照明能耗最小值
81	电源消耗主题	历史线网动力照明能耗平均值
82	电源消耗主题	每日能耗统计
83	电源消耗主题	每月能耗统计
84	施工管理主题	各施工单位计划分布
85	施工管理主题	各施工单位计划类型梳理
86	施工管理主题	计划兑现率
87	施工管理主题	施工类别统计
88	施工管理主题	各部门完成情况
89	施工管理主题	施工区域分布
90	施工管理主题	接报时间统计
91	施工管理主题	施工耗时统计
92	设备管理主题	重要故障
93	设备管理主题	故障修完成率
94	设备管理主题	计划修完成率
95	设备管理主题	各专业故障数
96	设备管理主题	各专业故障占比
97	设备管理主题	平均故障响应时间
98	设备管理主题	故障数 top5 站点
99	设备管理主题	每日各专业故障趋势

100	设备管理主题	每月各专业故障趋势
101	设备管理主题	每日平均故障响应时长趋势
102	总裁驾驶舱	累计运营里程
103	总裁驾驶舱	累计运营天数
104	总裁驾驶舱	累计开行列次
105	总裁驾驶舱	累计客运量
106	总裁驾驶舱	列车运行时刻表
107	总裁驾驶舱	当日正点率
108	总裁驾驶舱	当日各时刻列车开行情况
109	总裁驾驶舱	各站点实时客运量
110	总裁驾驶舱	当日实时客运量
111	总裁驾驶舱	当日票卡总收入
112	总裁驾驶舱	票卡类型数量占比
113	总裁驾驶舱	用电消耗图
114	总裁驾驶舱	线网牵引总能耗
115	总裁驾驶舱	线网每车公里牵引能耗
116	总裁驾驶舱	线网每人次牵引能耗
117	总裁驾驶舱	线网动力照明能耗
118	总裁驾驶舱	计划修完成比
119	总裁驾驶舱	故障修完成比
120	总裁驾驶舱	各专业故障占比
121	总裁驾驶舱	各部门计划分布图和兑现率
122	运营驾驶舱	累计运营里程
123	运营驾驶舱	累计运营天数
124	运营驾驶舱	累计开行列次

125	运营驾驶舱	累计客运量
126	运营驾驶舱	列车运行时刻表
127	运营驾驶舱	当日正点率
128	运营驾驶舱	当日各时刻列车开行情况
129	运营驾驶舱	各站点实时客运量
130	运营驾驶舱	当日实时客运量
131	运营驾驶舱	当日票卡总收入
132	运营驾驶舱	票卡类型数量占比
133	运营驾驶舱	用电消耗图
134	运营驾驶舱	线网牵引总能耗
135	运营驾驶舱	线网每车公里牵引能耗
136	运营驾驶舱	线网每人次牵引能耗
137	运营驾驶舱	线网动力照明能耗
138	总工驾驶舱	各施工单位计划分布
139	总工驾驶舱	各施工单位计划类型梳理
140	总工驾驶舱	计划兑现率
141	总工驾驶舱	施工类别统计
142	总工驾驶舱	各部门完成情况
143	总工驾驶舱	施工区域分布
144	总工驾驶舱	接报时间统计
145	总工驾驶舱	施工耗时统计
146	总工驾驶舱	重要故障
147	总工驾驶舱	故障修完成率
148	总工驾驶舱	计划修完成率
149	总工驾驶舱	各专业故障数

150	总工驾驶舱	各专业故障占比
151	总工驾驶舱	平均故障响应时间
152	总工驾驶舱	故障数 top5 站点
153	总工驾驶舱	每日各专业故障趋势
154	总工驾驶舱	每月各专业故障趋势
155	总工驾驶舱	每日平均故障响应时长趋势

4.4.2. 设备监测及运维类应用

设备监测功能贴近一线员工，侧重于设备的各类信息，使他们最直观地看到设备故障情况，及时定位故障位置，并对故障采取相应处理措施。从这点出发，设备监测的设计原则分三个层次：

- 1、 报警数据实时监测；
- 2、 与设备故障信息相匹配的维修建议、专家诊断方法；
- 3、 基于设备状态数据进行数据挖掘，给出预防性维修建议。

其中 2、3 已经是属于智能运维的范围。

设备监测设计的根本目标是“保证安全、提升效率、降低设备维修维护成本”。以此目标为出发点，根据智能化程度的不同，设备监测将运维分为了不同等级，大数据平台的远期建设目标应包含支持最高级别（GoM4 级）的运维场景。

各等级具体说明如下：

- 1、 GoM0-状态本地监测：各生产系统对自身系统内设备负责，监视系统内设备的状态信息，并进行本地化告警；
- 2、 GoM1-系统集中监测：在 GoM0 级基础之上，扩展远程监控手段，实现跨系统的集中设备状态监测。
- 3、 GoM2-数据互联可视：在 GoM1 级基础之上，加入了移动端管理和办公，同时加入关联数据 BI 展示，使得各系统运营数据能够为管理层提供决策支持。
- 4、 GoM3-智能诊断决策：在 GoM2 级基础之上，加入运维专家经验，使得各系统有可参照的可靠性数据模型，并据此进行智能诊断综合决策，为运营设备大幅提升 RAM 性能提供技术手段。
- 5、 GoM4-智能综合预测：在 GoM3 级基础之上，加入了设备健康模型，综合设备健康度模型和可靠性模型优化预防性维护建议，并通过运维结果自动调整模型参数，实

现运维体系的自动运行。

在设备监测方案设计时应建设地的信息化程度及现状、运营维护经验等进行深入的调研，并结合设备维修维护智能化等级，制定出符合建设地实情的设备监测方案，同时给出运维智能化建设规划建议。

建议设备监测设计方案短期建设目标对标 GoM2 级，通过数据共享平台，以实现各业务系统之间的数据互联与共享，打通业务系统之间的壁垒，在通过数据挖掘获得更多故障原因关联性的同时，也为中远期的智能运维创造了条件。

通过对信号、AFC 系统大量运转数据的实时监控收集和分析，检测故障征兆，在故障发生前进行预防保养，实现生产系统的最高效运转。

信号系统数据分析包含 ATS 子系统数据分析、转辙机工作数据分析、信号车载数据分析、信号系统车地通信质量数据分析及终端设备功能质量分析。

AFC 系统数据分析包含模式管理数据分析、设备监视数据分析、客流数据分析及票/款数据库分析。

4.4.2.1.信号系统数据分析

一、ATS 系统

通过数据共享平台采集到的前一日 ATS 明细数据进行统计汇总，展示以下数据指标：列车运行间隔、运行列车数、旅行速度、列车在各站实际到发时刻、列车早晚点、兑现率、正点率、加开列车数（临客、调试、回空、救援）、开行列车数统计、掉线列车数统计、清客列车数统计、延误运营事件数统计、列车服务可靠度统计、司机驾驶公里数统计。具体功能如下：

指标名称	计算逻辑	业务维度	功能点
列车运行间隔	根据当日计划运行图，统计列车运行间隔	线网、线路	
运行列车数	投入正线的列车数量	线网、线路	
旅行速度	每列车在运营线路正线上从起点站发车到终点站到达（将停站作业时间考虑在内）的平均速度	线网、线路	
列车在各站实际到发时刻	正线运行中，列车在各站的实际到站时刻和发车时刻	线网、线路	
列车早晚点	正线运行中，列车在各站的早晚点情况	线网、线路	
兑现率	实际根据计划开行车次（不包括加开车次）与运行图定开行车次之比	线网、线路	

指标名称	计算逻辑	业务维度	功能点
正点率	线路准点列车次数与线路实际开行车次数之比	线网、线路	列车早晚点不超过 1 分钟, 则认为准点列车
加开列车数	线路根据实际需要不在计划运行图内而增加开行的总列数, 包括临客、调试、回空、救援	线网、线路	
开行列数统计	列车为完成运营生产任务在正线上行驶的次數, 分为载客列次和空驶列次两部分, 包括计划外的加开车次	线网、线路	
掉线列数统计	统计凡因车辆及乘务原因, 致使列车未未完成计划运行图或运行方案所规定的任务的列车数	线网、线路	
清客列数统计	统计载客列车因各种原因, 未在计划运行图或运输计划规定的本车次终点, 发布调度命令将乘客由车厢清出的情况	线网、线路	
延误运营事件数统计	统计 5-15min 线路延误事件次数、15-30min 线路延误事件次数、30min 以上线路延误事件次数	线网、线路	
列车服务可靠度统计	线路列车发生 5 分钟及以上延误事件之间平均行驶的列公里数	线网、线路	
司机驾驶公里数统计	统计当日司机完成的列车运营里程数及其司机累计运行里程数	线网、线路	

二、转辙机

设定转辙机各参数的阈值门限, 对超限情况进行统计, 对超限数据进行深度分析, 结合专家经验库给出维修建议。以下为功能详情:

指标名称	计算逻辑	业务维度	功能点
道岔动作次数和时间	统计联锁系统中道岔动作次数和时间	设备	通过该次数推断道岔使用寿命并进行评估, 进而进行预报警
道岔动作时间超限统计	通过采集信号系统中的道岔动作时间, 统计汇总分析道岔动作次数中超过阈值门限的次数	设备	

指标名称	计算逻辑	业务维度	功能点
道岔动作电流超限统计	通过采集信号系统中的道岔动作电流，统计汇总分析道岔动作次数中超过阈值门限的次数	设备	
道岔表示缺口超限统计	通过采集信号系统中的道岔表示缺口数值，统计汇总分析道岔动作次数中超过阈值门限的次数	设备	
一启动继电器动作次数统计	通过采集信号系统中的道岔一启动继电器的动作次数或根据已知其他动作相关参数进行计算得出数值，统计汇总一启动继电器动作总次数	设备	
定反操继电器动作次数统计	通过采集信号系统中的道岔定反操继电器的动作次数或根据已知其他动作相关参数进行计算得出数值，统计汇总定反操继电器动作总次数	设备	
继电器动作次数统计	通过采集信号系统中的道岔表示继电器的动作次数或根据已知其他动作相关参数进行计算得出数值，统计汇总表示继电器动作总次数	设备	
一启动继电器动作时间统计	通过采集信号系统中的道岔一启动继电器的动作时间或根据已知其他动作相关参数进行计算得出数值，并对道岔一启动继电器动作时间设定阈值门限，统计汇总分析道岔动作次数中超过阈值门限的次数	设备	
定反操继电器动作时间统计	通过采集信号系统中的道岔定反操继电器的动作时间或根据已知其他动作相关参数进行计算得出数值，并对道岔定反操继电器动作时间设定阈值门限，统计汇总分析道岔动作次数中超过阈值门限的次数。	设备	

三、车载数据分析

对车载数据进行汇总统计并展示，可进行各线路、站点筛选。通过数据分析，结合专家经验库给出维修建议。需分析的指标如下表：

指标名称	计算逻辑	业务维度	功能点
ATO 停车精度	统计停车精度中单一列车的欠、过标信息，以及同一停车点的欠、过标信息，对列车/停车点进行维修	设备	给出维修建议
雷达故障码情况统计	雷达故障码出现时间、位置、速度跳变发生时间统计	设备	
速度传感器滑翔异常统计	速度传感器滑行异常出现时间、速度跳变出现时间、故障码发生时间	设备	

四、信号系统车地通信质量

对信号系统车地通信质量进行分析，对场强范围、超限时间、发生未知进行筛选，给出维修建议。分析指标详情如下表：

指标名称	数据来源	计算逻辑	业务维度	功能点
场强数值统计	数据共享平台	通过图形中正常值的设定来直观显示场强波动情况以及超出/低于正常范围的时间以及次数	设备	给出维修建议
红蓝网无线场强	数据共享平台	超限时间、发生位置统计	设备	

4.4.2.2.AFC 数据分析

对 AFC 设备进行监视，展示数据指标详情如下：

指标名称	计算逻辑	业务维度	功能点
AFC 设备故障情况统计	设备编号、状态编码、位置	线网、线路、站点	当监测到触发紧急模式时应发出报警，非运营时段内的紧急模式不用发出报警
储票箱内车票监视	统计车票余量	线网、线路、站点	数量不足或无车票的情况进行汇总统计并报警
合法移动涉及现金部件行为统计	合法移动涉及现金部件行为的记录统计	线网、线路、站点	非法移动涉及现金部件行为的记录进行汇总统计并报警

指标名称	计算逻辑	业务维度	功能点
车站车票库存监视	统计车站车票库存	线网、线路、 站点	设定车票库存阈值，当库存低于或超出阈值时，系统进行汇总统计并报警
设备使用次数	对设备使用次数进行统计	线网、线路、 站点	在设备寿命结束前发出报警提示

5. 基础设施配套设计

传统机房一般采用工业空调对机房整体空间制冷的方式，因为没有很好地考虑用电、制冷、气流管理的问题，PUE（Power Usage Effectiveness，能源效率指标）偏高，传统机房的PUE都在2.0以上甚至更高。即所使用的能源约有一半消耗在IT设备上，另一半消耗在包括电源设备、冷却设备和照明设施在内的物理基础设施上。

云平台是信息化系统的基础平台，是需要随着城市城轨系统的发展而进行扩展的。机房建设作为支撑云平台的底层架构，需要能根据云平台的需求而扩展。使用传统机房的建设模式，实现快速部署、按需扩展均比较困难。

作为城轨云的机房，应能体现快速部署、灵活扩展、绿色节能的技术特点。

5.1. 机房设备布置的设计原则

按照GB50174-2017《数据中心机房设计规范》，数据中心等级可分为A、B、C三级：

- 1) A级为容错型，其场地设备不应因操作失误、设备故障、外电源中断、维护和检修而导致电子信息系统运行中断
- 2) B级为冗余型，其场地设备在冗余范围内，不应因故障设备而导致电子信息系统运行中断
- 3) C级为基本型，保证电子信息系统运行不中断

城轨云中心机房的等级应为B级冗余型，建议主用中心可按照不小于300平进行规划，机房面积可以满足3条线路全业务系统上云的要求，机房中根据具体设计确定是否包含配套精密空调及UPS设备。

城轨云机房一般采用机柜上走线部署线缆，有助于提高机房的可靠性和可用性。面对大量的线缆，便于检修维护和线路调整，同时便于线缆散热，尤其针对电力电缆。由于地板下没有大量线槽等遮挡物，便于空调送风。有利于机房内温湿度分布更均匀，降低空调负载，同时便于直接观察到明火、烟雾等，有利于防火安全。

机房设备的布置须根据设备的多少，扩展性的要求，来规划模块化机房的规模和布局。须根据供电及制冷条件确定是采用低密度布局（5KW/机柜）还是高密度布局（10KW/机柜）。如果机房空间够，可以采用低密度布局搭配精密空调方式。如果机房空间紧张且供电有保障，可以采用高密度布局搭配列间空调方式。

机房设备布置宜遵循逻辑网域划分的原则。在条件允许的前提下，安全生产网、内部管理网、外部服务网、运维管理网应部署在不同的模块化机房内。如条件允许，可考虑同网内的IT设备（服务器、存储）与网络设备（交换机、防火墙）分别部署在独立的模块化机房内，便于日后扩展。运维管理网可根据情况和其它区域合设。

同一模块化机房内须有逻辑分区，如 IT 设备中裸金属、云主机、云桌面主机、存储、云管理系统、备份系统应分布在不同机柜内。如使用集中存储系统（如 FC SAN 或 IP SAN），存储系统宜部署在 IT 设备中央位置，减少存储走线的长度。对于网络设备，核心交换机宜部署在中心位置，核心防火墙，IPS 等设备依次部署。

机柜内布线应宜采用结构化布线方式。跨 1 个以上机柜的线缆宜通过配线架进行连接。服务器机柜最多配置 3 种配线架，分别用于接存储、接业务网络、接带外管理。存储系统、业务核心交换机，宜配集中配线柜。

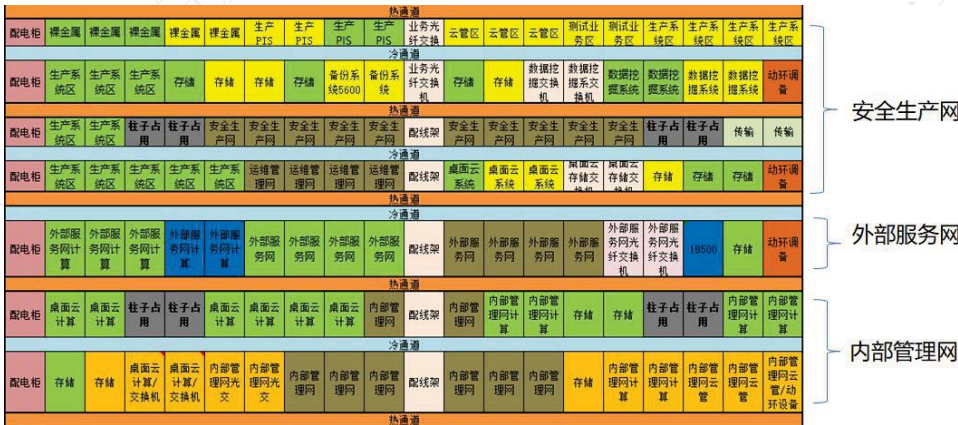
城轨云机房须为系统未来的扩展保留空间。对于网络设备，应预留出相应的端口或卡槽位。对于 IT 类设备，应在模块化机房内适当预留扩展用机柜。扩展用机柜内宜提前安装好所需 PDU、配线架等设备，后续新设备安装后可快速投入使用。

数据中心机房常采用物理基础设施资源池 POD (Point Of Delivery) 方式交付，POD 基于容量和应用进行设计，通常由两排对称的机柜组成。在实际部署中，一个 POD 跟一个模块化机房为同一概念。

5.2. 机房设计

5.2.1. 主用中心布置方案及呼和浩特云平台实例

城轨云平台主用中心分为 4 个网域（3 个业务域 + 1 个管理域），机房机柜的设计建议与网域一致，将安全生产网、内部管理网、外部服务网、运维管理网物理分开。其中，安全生产网、外部服务网因包含业务系统，会随承载线路的增多而需要扩容，在设计机房时须考虑扩容的空间需求。内部管理网内的业务相对稳定，对资源的占用率相对较低。建议初期规划时预留部分资源（机柜空间、供电、端口等），用于未来业务扩容和新业务上线。



以呼和浩特城轨云为例，呼和浩特城轨云平台主用中心机房 410 平米，机房内包含了云平台模块化机房及精密空调系统。使用整体 UPS 方案，云平台机房不包含 UPS 设备。

整个平台共有 3 个半模块化机房，一个模块化机房包含 40 个机柜（20*2 列，承重柱占用

两个柜位），每列包含 1 个配电列头柜、19 个设备柜。其中的半个模块化机房，仅包含 1 列 20 个机柜，另外半列使用玻璃封堵闭合。采用低密度布局方式（单柜 < 5kw），采用地板下送风的方式。配电列头柜使用 A、B 两路供电，单路电功率 60kw（第一期工程）。

3 个半模块化机房中，安全生产网占 2 个模块，内部管理网占 1 个模块，外部服务网占半个模块，运维管理网与安全生产网共柜。因呼和浩特云平台外部服务网承载业务有限，使用半个模块已能满足需求。如在其它城市实施，可根据实际设备进行设计和分配。

安全生产网分配了 2 个模块化机房，1 个模块主要部署 IT 设备，另 1 个模块主要部署网络设备。在 IT 设备模块，将 SAN 光纤交换机布置在列中，存储设备尽量靠近光纤交换机。其余空间，按照虚拟机服务器（2 联柜部署）、裸金属服务器（2 联柜部署）、云管理系统、数据挖掘系统进行分别部署。在网络设备模块，将配线架布置在列中，两侧依次部署核心网络设备。其余空间根据可用的机柜分别部署云桌面系统、运维管理网络，互联所需传输设备等。

内部管理网和外部服务网结构相对简单，可采用统一的布置原则。将配线架布置在列中，两边部署网络设备。再根据剩余空间部署虚拟机服务器（2 联柜部署）、裸金属服务器（2 联柜部署）、存储系统、云桌面系统等。

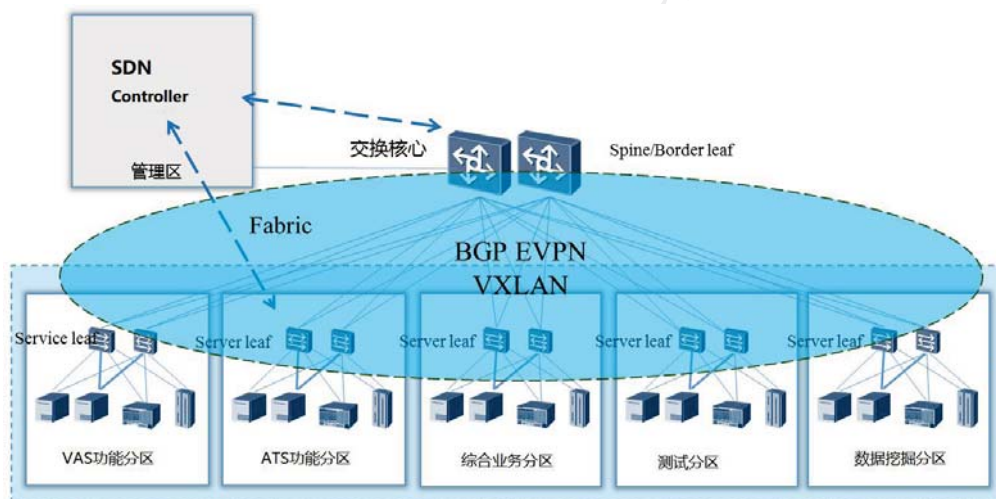
5.2.2. 网络设备布置原则

城轨云网络依赖于 SDN（Software Defined Network，软件定义网络）架构。建议使用硬件 SDN 方案，即使用专用的硬件交换设备与控制器来实现相关的网络功能，控制器对硬件设备进行策略以及流表的下发，来实现网络相关的功能。

随着虚拟化的发展，与之配合的新的网络设计已经从原来的三层结构（接入-汇聚-核心）逐步演进成两层架构（Fabric + Leaf-Spine）。服务器接口速率 10GE 以上，接入交换机上联速率 40GE 以上。10GE 网络光端口多采用 LC 类型的端口连接器件，对于 40GE/100GE 网络光端口建议采用 MTP/MPO 接口方式。

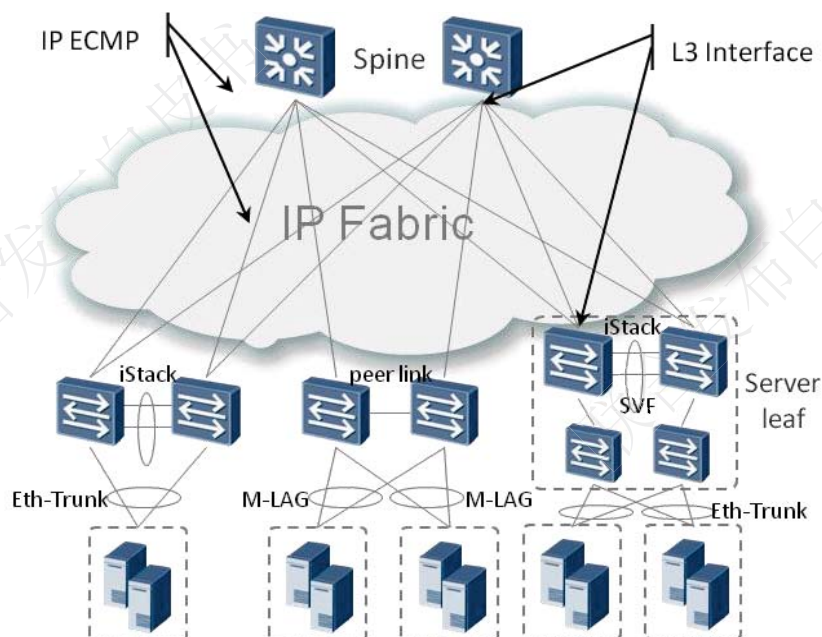
5.2.2.1. 城轨云网络结构与 SDN 设置

城轨云建议每个业务网域设置独立的 OpenStack 控制节点及 SDN 控制节点。在一个 SDN 控制节点下，各个业务区共享一个网络资源池，提升网络设备的利用率。这个网络资源池称为 Fabric。通过 VXLAN 技术，网络被解耦为两层，即 Underlay 网络和 Overlay 网络。Underlay 网络是真实物理网络连接，Overlay 网络为虚拟化网络。在设计机房时应结合 Underlay 网络的规划，充分考虑城轨云平台的网络特点，进行针对性设计。



在 Underlay 的物理网络架构中，多采用叶脊（Spine-Leaf）的二级结构，Spine 和 Leaf 之间为全网状连接（Full Mesh）。安全生产网通常使用 2 台核心交换机作为 Spine 节点。Server Leaf 即为业务接入交换机，可接入虚拟化服务器、裸金属服务器、桌面云服务器。Service Leaf 根据项目实际情况配置，若无 VAS 设备，则可不设 Service Leaf 节点。

平台还需跟大量的传统网络做对接，非云接入交换机、终端汇聚交换机、线路汇聚交换机可以不属于 SDN 的范围，需手工配置，可不靠 SDN 控制器进行策略和流表的下发。SDN Underlay 网络通常包括核心交换机（Spine 节点）、业务接入交换机（Server Leaf 节点）和核心防火墙。



呼和浩特城轨云 Underlay 设计：

呼和浩特城轨云采用 Border Leaf 和 Spine 合一的方案，架设 2 台核心交换机，既作为 Border

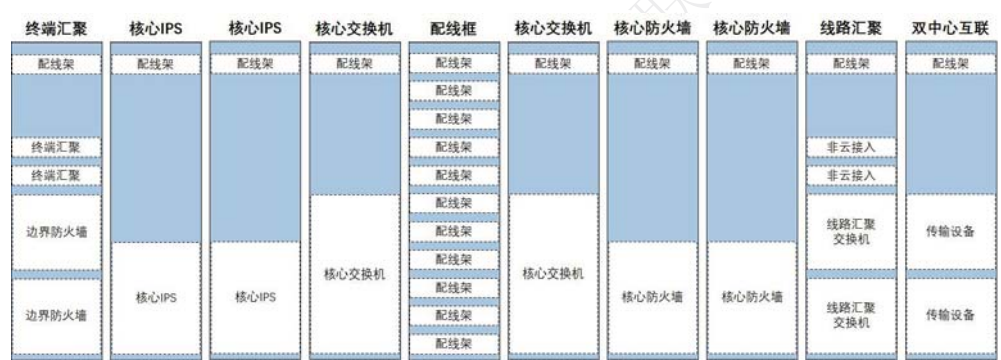
leaf（还兼做 VXLAN L3 网关），又作为核心转发节点 Spine。Spine 节点同 Leaf 节点相连的以太网口配置为三层路由接口，构建 IP Fabric 网络。

Leaf 节点同每个 Spine 节点相连构建全连接拓扑。同时 Leaf 节点作为 Underlay 网络的 L2/L3 分界，同 Spine 节点相连的以太网口配置为三层路由接口。Leaf 节点即为计算设备内的 TOR 业务接入交换机。

5.2.2.2.网络设备布置及布线

根据整体机房要求，城轨云网络宜采用结构化布线方式，即在服务器端口与接入层交换机之间采用水平缆线+配线架进行布线，接入交换机与核心/汇聚交换机之间采用主干光缆+配线架进行连接，通过配线架跳线分别跳至交换机端口和设备端口。由于柜间配线架的通道在平台建设期间已做好预留，仅增加柜内设备至配线架的布线施工即可实现后续线路接入安全、快捷。

核心网络设备布置示意图如下：



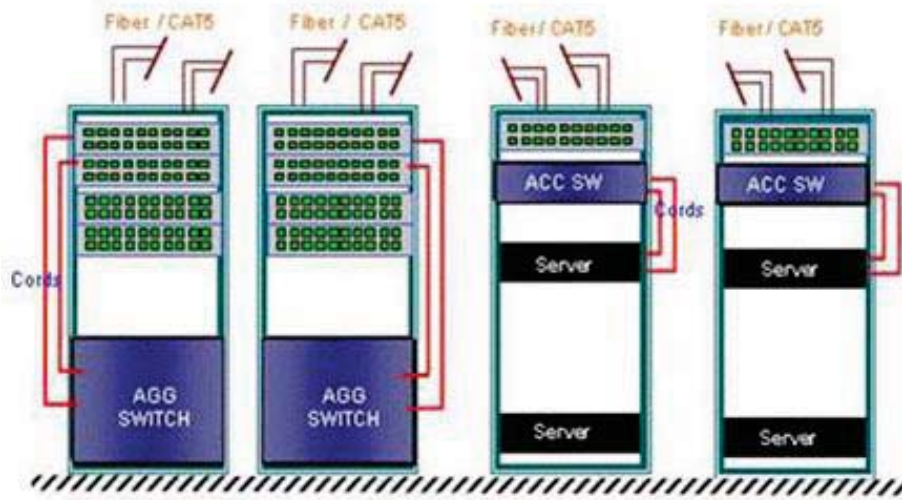
核心网络设备应部署在整个网域的中心位置，使到各机柜的线缆距离最短。中心配线架部署在最中心，从 Leaf（业务接入交换机）过来的缆线在此成端。核心交换机分列中心配线架两侧，两侧再依次排列核心防火墙、核心 IPS、线路汇聚、终端汇聚、非云接入、主备中心互联设备。

设备的布置须考虑单机柜最大承载功率，如果采用低密度机柜（单机柜< 5kw），可能存在单个设备功率较大，放置单台设备后无法再部署其它设备的情况。

5.2.3. 计算设备布置原则

5.2.3.1.接入交换机 TOR 部署

呼和浩特城轨云采用的是交换机 TOR 布线方式，采用 TOR 布线时，POD 中每个服务器机柜的上端部署 1-2 台接入交换机，机架式服务器通过跳线接入到机柜内的交换机上，交换机上行端口通过线缆接入到平台的汇聚交换机或核心交换机上。如图所示：



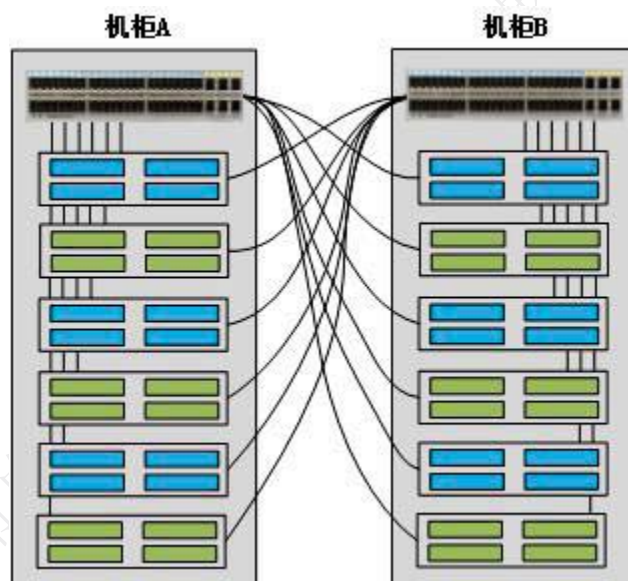
(图片源自网络)

TOR 布线方式简化了服务器机柜与网络机柜间的布线，从每个服务器机柜到汇集交换机与核心交换机网络机柜的光纤或线缆数量较少（4-6 根），有利于在一个机柜内部署更多的服务器。对于高密度机柜，如果采用交换机 TOR 布线方式，每个机柜在部署 15-30 台机架式服务器依然能保证线缆数量可控。但对于低密度机柜，受电源输出功率限制，可部署的服务器数量有限，可能会出现服务器机柜内交换机的接入端口利用率不足的现象。

从网络设计考虑，TOR 部署方式的接入交换机数量会比传统方式要多，网络设备管理维护工作量要大。城轨云规模较大，且有很强的扩展性需求，在城轨云中心机房部署推荐使用接入交换机 TOR 部署方式。

5.2.3.2. 计算设备两联柜部署

呼和浩特城轨云的计算资源是采用两联柜方式部署，两台机柜上分别部署一台 48 端口 TOR 交换机，每台交换机的 24 个端口提供本机柜的服务器接入，另外 24 个端口提供给相邻机柜的服务器接入。根据项目实际配置情况，每个 TOR 交换机与服务器建议采用 10G/25G 的光纤连接，上联至汇聚/核心交换机建议采用 40G/100G 光纤连接。上联光纤建议首先跳至柜内配线架，柜内配线架至汇聚/核心配线架的光纤须预置并成端，再从配线架跳至汇聚/核心交换机。扩容计算能力，如需新机柜，也应以两联柜方式扩容。



(图片源自网络)

5.3. 模块化机房

传统机房一般采用工业空调对机房整体空间制冷的方式，因为没有很好地考虑用电、制冷、气流管理的问题，PUE（Power Usage Effectiveness，能源效率指标）偏高，传统机房的PUE 都在 2.0 以上甚至更高。即所使用的能源约有一半消耗在 IT 设备上，另一半消耗在包括电源设备、冷却设备和照明设施在内的物理基础设施上。

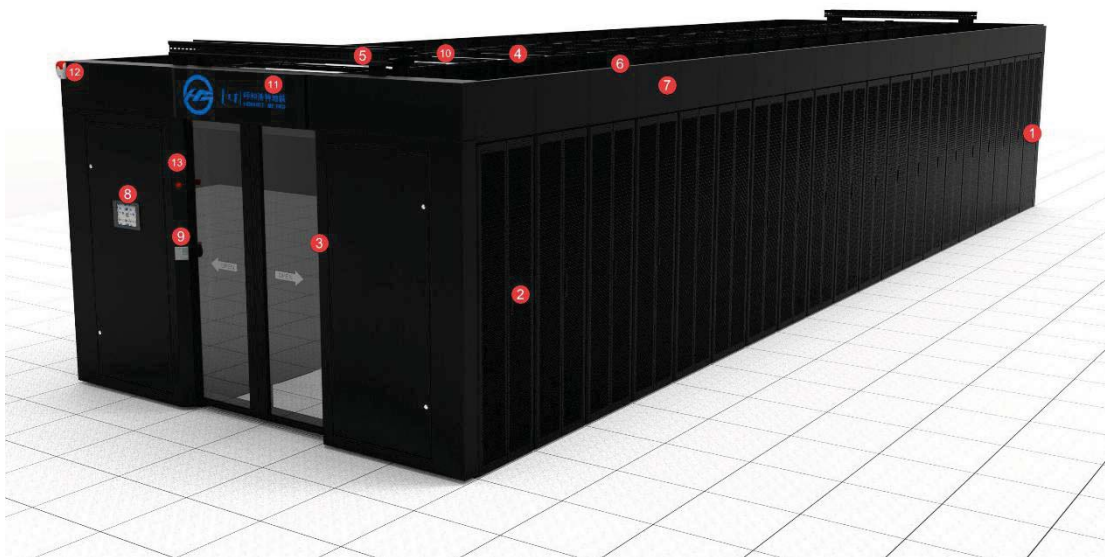
城轨云平台是信息化系统的基础平台，是需要随着城市城轨系统的发展而进行扩展的。机房建设作为支撑云平台的底层架构，需要能根据云平台的需求而扩展。使用传统机房的建设模式，实现快速部署，按需扩展比较困难。应采用模块化机房，能体现快速部署，灵活扩展，绿色节能的技术特点。

模块化机房还有以下优点：

- 1、 模块化：冷通道封闭采用为模块化设计，冷通道两侧相对应的两台机柜为一个模块。每个模块均能独立安装与拆卸，方便用户增加、减少或者移动通道内部分机柜。
- 2、 安全性：每个顶板均可实现与消防联动。当模块化机房内火灾信号确认后，顶板自行打开，消防灭火气体可以进入通道灭火。
- 3、 安装：安装简单，不会破坏模块化机房现有装修，安装现场不用动火烧焊。在机房和布线工程技术规范文件中，对布线工程实施要求机房内强、弱电走线应明显分开，以避免电磁干扰。一般要求强电采用地板下走线，弱电采用上走线，强电采用线槽，弱电采用吊装金属梯架。

5.3.1. 模块化机房简介

模块化机房包含机柜、配电和监控等功能单元，模块全部组件可在工厂预制，并可灵活拆卸，快速组装，与建筑实现解耦，以工程产品化实现快速部署，在较短时间内实现高质量的标准化交付，并大幅降低建设成本。



（图中：(1)配电列头柜 (2)设备机柜 (3)冷通道端门 (4)天窗 (5)列间跨线桥架 (6)M 线槽 (7)顶置围板 (8)本地监控单元 (9)门禁读卡头 (10)通道照明系统 (11)LOGO 标识灯箱 (12)声光报警器 (13)紧急按钮）

5.3.2. 冷通道/热通道

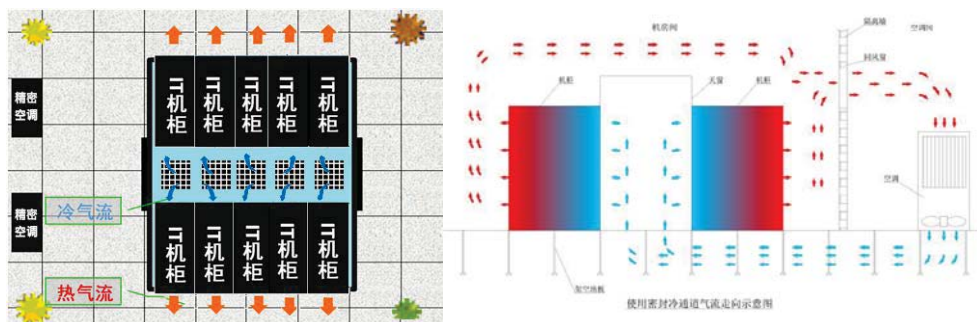
机柜采用“背靠背、面对面”摆放，这样将两排机柜的正面面对通道区域进行封闭，冷空气从通道封闭区域的通风地板吹出，封闭区域形成一个冷空气区“冷通道”，冷空气流经设备后形成的热空气，排放到两排机柜背面中的“热通道”中，热空气回到空调系统，使整个机房气流、能量流流动通畅，提高了机房精密空调的利用率，进一步提高制冷效果。从整个机房的气流组织来看，有效地避免了传统机房中冷热空气混合，冷空气短路，以及远端机柜由于压降的问题，导致的机柜顶端设备无足够冷量用于散热，最终产生的局部热点问题。



5.3.3. 制冷方式

1、 架空地板下送风制冷

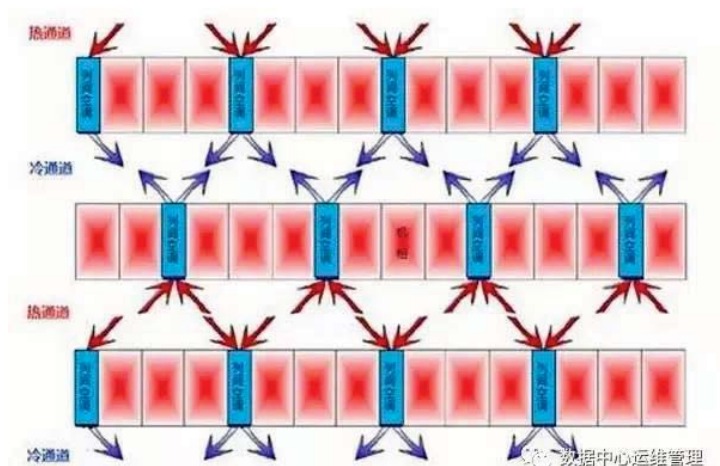
架空地板下送风方式在机房净高比较充裕的情况下才能考虑。精密空调通过地板下空间送风。需要在模块机房通道内的地板上开孔，将地板下作为一个静压箱。冷气流自下而上进入冷通道，穿过机柜进入热通道。再由热通道统一向空调回风。



(图片源自网络)

2、 列间空调整冷

列间空调，是放在服务器机柜列间，热源直接散热的设备，为水平送风机组，主要应用于高热密度数据中心。列间机房空调的设计，冷风是从冷通道送风，后由热通道回风的水平送风方式，从而完全解决了冷热气流短路的问题，保障了服务器机柜温度的均匀，消除了局部热点，进而增加了服务器的运行可靠性同时有效的降低了不必要的能耗。



(图片源自网络)

5.3.4. UPS 供电

1、 正常运行

UPS 正常运行状态，即 UPS 输入市电正常，整流器和逆变器均正常工作，负载由逆变器供电，电池开关闭合且电池在直流母线电压下处于稳定的浮充状态，

注意：由于并机系统（“1+N” UPS 并机系统）中各 UPS 单机的输出必须并联在一起，所以系统会检查各逆变器控制电路是否同步，以及与市电旁路的频率及相位是否完全吻合，同时还要保证它们各自的输出电压完全相同。负载的供电电流自动由各 UPS 单机均衡承担。在同步过程中，UPS 系统会显示相应的警告信息。

2、 市电异常

如市电停电或不正常，整流器将自动停止工作，系统转由电池逆交输出。电池逆交时间的长短取决于负载的大小及电池的容量。在此期间，如电池电压下降至放电终止电压且市电仍未恢复正常，逆变器将自动停止工作，UPS 的操作控制显示面板将显示相应告警信息。（市电的中断和恢复都不会中断对负载的供电）。

3、 市电恢复

当市电在允许的时间内恢复正常时，整流器将自动启动（此时其输出功率逐渐增加），重新给逆变器供电并对电池进行充电，因此负载的供电不会中断。

4、 电池脱离

如需将电池从 UPS 系统脱离以备维修，可通过外部隔离开关将电池分离，此时，除不能具备市电停电时的电池后备功能以外，UPS 的其它功能及规定的所有稳态性能指标均不受影响。

5、 UPS 单机故障

如出现逆变器故障，负载自动转由旁路供电，输出电源不会中断。如并机系统中的某个单机发生故障，该单机将自动退出并机系统，如系统中剩余的单机仍能满足负载的供电要求，系统将继续给负载供电，负载电源不中断。如果剩余的单机不再能够满足负载的供电要求，负载将自动被切换到旁路市电。

5.3.5. 消防联动

云平台机房设备支持与消防系统进行联动。当机房发生火灾时，消防系统或烟雾探测器输出信号至机房动环系统监控主机，动环系统发出声光报警同时消防控制主机也会发出信号使得天窗立即反转打开，翻转式天窗可开启部分面积达天窗面积的 85%，以利于消防气体能够快速进入通道内。

5.4. PUE 计算

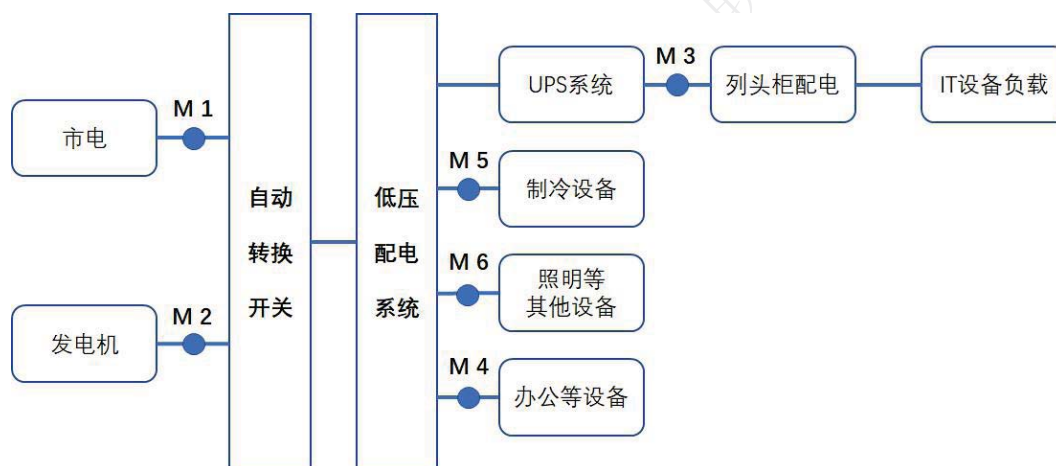
5.4.1. PUE 指标测量点

为计算 PUE，需要在下图所示的数据中心的供配电系统示意图中，测量数据中心总耗电及 IT 设备耗电，具体测量点如下：

- 1、 数据中心总耗电在正常情况下，数据中心的电能由市电提供，测量点应取市电输入变压器之前，即图中的 M1 点。当市电故障情况下，柴油发电机产生的电力（图中 M2 点）作为数据中心总耗电的测量点。如果是多用途机房楼，数据中心总耗电计算中，需减去在 M4 点测量的办公等其他耗电。
- 2、 IT 设备耗电严格来说，IT 设备耗电应该在各 IT 设备输入电源处测量耗电量并进行加总，但由于 IT 设备数量较多，这一方法将大大增加测量工作量和成本。因此，在实际操作中，可在各路 UPS 输出或者列头柜配电输入处进行测量后，将测量值加总作为 IT 设备耗电。每一路供电的 IT 设备测量点即图中的 M3 点。

确定测量点之后，根据定义 PUE 的计算方法：

$PUE = (P1 + P2 - P4) / P3$ 其中 P1 为在 M1 点测得的用电量，依此类推。



PUE 指标的测量点

计算 CLF 和 PLF 指标，需要在 PUE 测量点的基础上，增加制冷设备耗电、照明等其他设备耗电的测量点，即图中的 M5、M6 点。

$$CLF = P5 / P3$$

$$PLF = (P1 + P2 - P3 - P4 - P5 - P6) / P3$$

另外，还需要注意数据中心总进线开关柜、列头柜或电子信息设备终端配电装置宜安装有功电度计量装置。当列头柜内安装有隔离变压器时，有功电度计量装置的计量不应包括隔离变压器的损耗。当数据中心位于其他建筑物内时，数据中心总用电量中不应包含其他功能用房的用电量。数据中心使用的有功电度计量装置应具有用电量显示、累积和信息传输功能。

检测用仪器仪表应符合下列要求：

- 1、有功电度表的精度等级不应低于 1.0 级；
- 2、交流电压/电流互感器的精度等级不应低于 0.5 级。PUE 电能利用效率的检测应长期连续进行，当电能利用效率的数值小于本地区数据中心平均电能利用效率时或小于自身以往历史数据时，可判定数据中心达到节能。

5.4.2. 能耗的间接测量和估算

在实际测量中，部分需要的耗电量可能无法直接测量得到，而应通过一定的方法进行间接测量和估算。

能耗指标的数值受各种因素的影响，会随季节、节假日和每天忙闲时段的改变发生变化，因此为全面、准确了解数据中心的能效，应采用固定测量仪表，对数据中心能耗进行持续、长期的测量和记录。如果没有固定测量仪表，测量的周期和频率应：

- 1) 建议每次测量时间不小于 1 小时；
- 2) 建议每天测量不少于 2 次，在业务忙时和闲时进行测量；

- 3) 建议每月不少于 3 天，如可在 5 日、15 日、25 日进行测量。数据中心应根据连续或多次短时累计的数据中心总耗电、IT 设备耗电等测量值(单位为 kWh)来计算 PUE 等能效指标。

6. 城轨云测试平台

6.1. 设计原则

城轨云平台测试平台整体按照“硬件最小化，功能最大化”的最小系统的思想，提取城轨云平台系统中的核心设备和典型设备作为最小系统的雏形，选取功能和接口全覆盖的最小子集作为最小系统的首选模型，采用功能接口全部预留和增量式的整体架构，按照云平台主用中心安全生产网、外部服务网、灾备中心安全生产网构建仿真测试平台架构，模拟城轨云平台系统各种运营场景，并满足城轨云平台测试大纲的验证测试。

城轨云测试平台可分为在线测试平台和离线测试平台两种形式，其中在线测试平台使用正线平台划分测试区域方式，可负责接口测试、大数据测试、业务升级测试与接入测试；离线测试平台通过独立于正线云平台搭建，负责云平台升级验证、性能测试和压力测试。从呼和浩特城轨云测试平台的搭建经验来看，使用独立的测试平台会比正线平台上分出一个资源区域更有利于进行性能、压力测试和验证工作的开展。原因如下：

1. 测试平台可能需要验证底层云平台升级流程，这种高危类型的操作必须使用独立测试平台。
2. 为了满足测试要求，测试过程可能需要对试验环境进行调整。使用独立测试平台能有效减少对生产环境的影响。

呼和浩特城轨云设计规划设置在线测试平台，但其具备使用条件的时间较晚，不满足项目测试时间节点要求，使用在线测试区域进行测试达不到提前验证云平台、业务系统及其兼容性的目的，故呼和浩特城轨云测试平台主要采用离线测试平台的形式进行测试。

测试平台的设计应遵循如下原则：

1. 在主用中心保留了安全生产网（含中心及站段）、外部服务网和运维管理网结构
2. 除主用中心安全生产网核心交换机及防火墙外，其它设备均无冗余设置
3. 仅验证基础安全功能，包括：核心防火墙和核心路由器的联动、审计及漏洞扫描
4. 中心互联、站段互联不使用传输，使用交换机直连模拟

收集业务系统资源需求，计算硬件需求遵循如下原则：

1. ATS、ISCS、AFC、PIS 业务系统容量满足半实物测试平台需求
2. 资源容量满足各业务系统同时进行功能测试
3. 资源容量满足任一业务系统全线或全网性能测试

因呼和浩特 1、2 号线的综合监控、PIS、PBE 均为一家供应商，1、2 号线门禁 ACS 都汇总到一个中心平台上，测试平台不再进行 1、2 号线系统的区分。因测试平台未设置内部管理网，信息化系统部署在测试平台的安全生产网，仅用于上云的兼容性及功能测试。

就呼和浩特城轨云 2 条线的测试平台实践经验来看，整个测试平台资源规划约为主用中心安全生产网资源的 60%左右。因不涉及内部管理网，仅涉及少量站段、简化的安全设备以及灾备中心，整个测试平台不应超过整体规模 30%。

业务系统资源分配表

业务名称	vCPU / 个	内存 / G	存储 / G	裸金属
1 号线 ATS	178	392	14600	1
2 号线 ATS	72	140	1800	1
综合监控	516	1216	25288	3
1 号线 AFC	12	24	900	2
2 号线 AFC	248	560	12000	
PIS	288	448	7200	
1 号线 CAS	24	40	2000	
2 号线 CAS	24	24	1500	
PBE	32	160	4000	
信息化	136	272	7200	
门禁 ACS	52	104	2800	
大数据平台	80	160	5000	3

通过城轨云平台测试平台的搭建，不仅可展现城轨云平台系统最先进技术及最新成果，同时还可以达到以下目的：

1. 城轨云平台技术原理演示

通过该城轨云平台测试平台，可以动态展示城轨云平台创新技术。提供风格统一的展示界面。

2. 城轨云平台技术及设备的测试与验证

对城轨云平台测试平台系统设备样机的需求符合性进行验证。

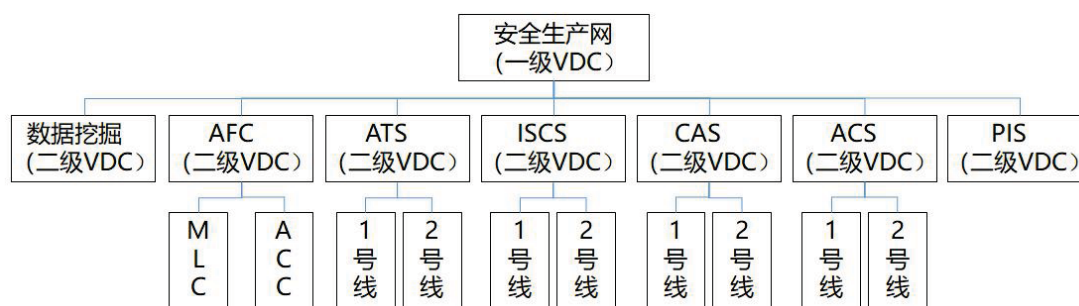
3. 城轨云平台全系统、全功能集成验证平台

验证城轨云平台测试平台系统功能、性能要求的符合性，并为安全评估与认证、上线运行提供支撑。

6.2. 测试平台设计

城轨云测试平台设计时充分考虑模拟城轨云平台系统各种业务场景，并满足城轨云平台测试需求。

1. 明确测试范围：考虑远期接入的各业务系统。
2. 完成网络架构规划：根据各业务的网络接入数量及规格确定光电模块、百千万兆网络交换机的配置。
3. 制定模块化的平台系统：依靠 VDC 进行模块分割，将各业务系统应用、各业务系统仿真软件进行整合。
4. 远期功能：预留其他业务系统接入测试平台的能力。



测试平台 VDC 划分

为达到通过测试平台验证云平台设计方案正确性，尽可能保持测试平台与运营平台一致。

云测试平台与主用中心架构一致性：

1. 均具备主用中心和灾备中心双中心结构
2. 主用中心安全生产网核心交换机及防火墙均采用冗余配置，防火墙采用旁挂核心交换机方式

3. 测试平台网络架构基本与主用中心一致

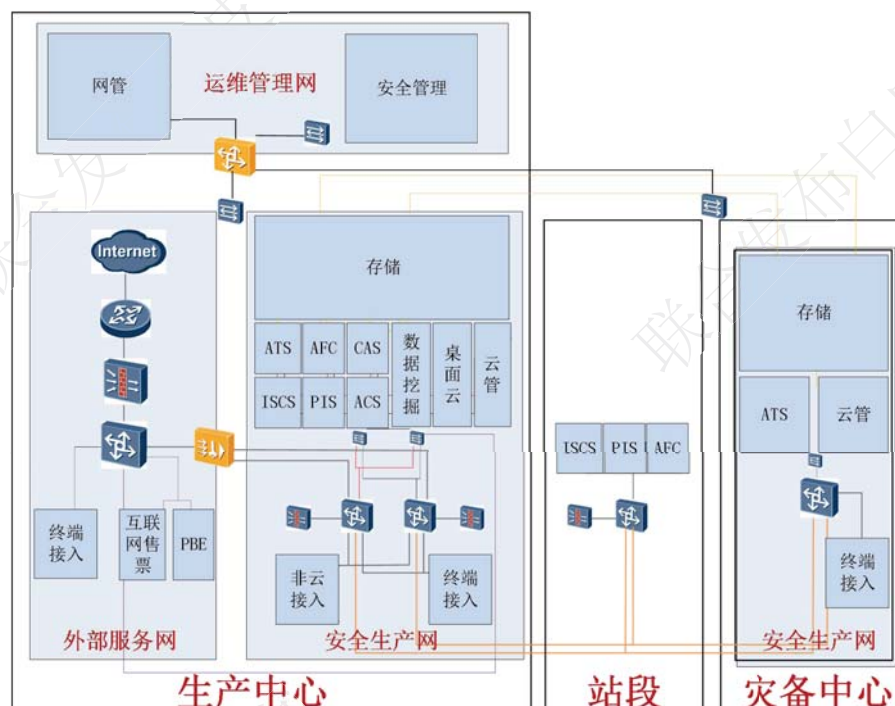
云测试平台与正式部署一致性：

1. 测试平台 VDC 划分原则与主用中心一致
2. 资源分配与主用中心一致

3. IP 配置与主用中心一致

云测试平台业务系统一致性:

1. ATS、ISCS、AFC、PIS、ACS、CAS、大数据平台及信息化 OA 均上云部署
2. 部署的业务系统为主用中心使用的业务软件及数据
3. 站段采用虚实结合方式进行，真实设备按 1 个标准站配置，提供站段接入交换机供各业务系统真实设备接入，其他车站采用虚拟化部署。



城轨云平台测试平台部署架构

云测试平台搭建完毕后，具备以下特点：

1. 集成度高

此测试平台为可验证城轨云平台系统关键组成部分及功能的最小系统测试平台。并且统一资源池、统一数据源存储，提高系统利用率。

2. 完整度高

可支持多系统联调、接口测试、主备中心测试的不同需求。

3. 深度整合

接入各业务系统自身的仿真平台，统一分配业务仿真区，通过 SDN 组件完成网络配置，进一步提高系统利用率。

4. 模块化

可根据不同项目的不同阶段进行不同模块的测试。

5. 覆盖面广

可根据不同项目需求测试单中心/双中心互连、网络 SDN 配置、多集群协同调度、不同云管、云桌面、安全、存储系统异构等一系列测试。

6.3. 测试范围

云测试平台搭建完毕，进行云平台自测试、业务系统功能及兼容性测试、性能测试和灾备测试。

6.3.1. 云平台自测试

云平台自测试内容主要包含运营管理、云服务、运维管理、云桌面四个方面及云平台故障类测试、灾备测试，验证搭建完成的云测试平台 VDC 创建、用户创建、子网创建、申请弹性云服务器、注册镜像、云硬盘服务、系统资源监控、报表查询、云桌面等各项功能实现情况，以保证满足具备业务系统上云部署测试的条件。

6.3.2. 业务系统功能及兼容性测试

业务系统功能及兼容性测试通过验证业务系统部署至云平台后业务系统各项功能满足设计要求，业务系统在云平台运行正常进行测试。

对于信号系统 ATS 测试，执行 ATS 界面元素显示、进路办理、运营计划加载、自动分配车次、列车详细信息显示、遥控站控控制功能验证、扣车跳停、主备切换等功能测试，以判断 ATS 软件在云平台运行正常，与平台兼容性满足要求。

对于综合监控 ISCS 系统，执行综合监控通用功能、控制权移交、单遥功能、顺控功能及与其他业务系统交互功能，进行 ISCS 能源管理和信息安全功能模块测试，验证 ISCS 在云平台上运行稳定，与云平台兼容性满足要求。

自动售检票 AFC 主要执行 AFC 通信连接、控制命令、账户管理、状态上传、模式下发、参数同步等功能测试，验证 AFC 软件功能具备，与云平台兼容性正常。

门禁系统 ACS 执行线网平台登录、操作员管理、线路接入、数据接入、持卡人管理、远程控制等相关功能测试，验证本线网云平台 ACS 系统各项功能需求及与云平台兼容性满足要求。

乘客信息 PIS 系统执行设备监测、系统管理相关测试、播表软件功能测试、组播功能测试、与综合监控功能测试、与信号系统功能测试、与集中告警功能测试，验证 PIS 与云平台测试验证功能点具备。

公务电话 PBE 系统执行综合接入设备测试、网管功能测试、计费功能测试、PBE-CAS 接口测试、测试 PBE 功能、与云平台兼容性是否符合技术标准及相关文件要求。

集中告警 CAS 系统执行故障管理功能测试、故障分析功能测试、安全管理功能测试、配置管理功能测试、拓扑管理功能测试、告警通信测试，验证云平台 CAS 测试验证功能点具备。

6.3.3. 系统性能测试

系统性能测试包含两部分，分别为云平台虚拟机性能测试和业务系统性能测试。

云平台虚拟机性能测试针对云平台内分配的虚拟机进行磁盘读写、网络带宽、丢包率等性能指标进行测试，判断云平台自身是否满足性能要求。

业务系统性能测试主要针对业务系统压力测试时系统运行状态及分配资源使用情况进行确认，判断资源分配是否满足业务系统需求。

业务系统性能测试方法

测试类别	业务系统	测试方法
性能测试	ATS	模拟 24 辆以上列车 2 分钟间隔跑图，系统按计划运行 10 小时以上并绘制实际运行图，各列车站台作业正常，停站时间响应正常，追踪运行正常。
	ISCS	针对历史服务器中存储的综合监控数据，包括历史事件、趋势、报表，导入导出不同规模大小的数据量，记录和分析耗时性能。基于工程数据组态 50 万 I/O 点，且中心服务器部署 20 万点、车站服务器部署 10 万点，FEP 部署 1 万点，对 HMI 和实时服务启动时间、切图时间、HMI 读写数据时间等性能进行测试。对综合监控常用的业务场景进行长时间拷机压力测试，以及对服务器部署数据点总数的 20%、40%和 80%的点进行随机模拟。
	AFC	估算每日客流量及早晚高峰数据，对各项业务进行高低并发压力测试，分析各设备性能、数据吞吐量以及稳定性。
	ACS	平台下发 1 万个以上持卡人到线路服务器，查看每台服务器的运行情况。
	PIS	在 ISCS,ATS 进行性能测试时，将数据同步接入 PIS，测试编播中心、线网中心、车站、车载各功能正常运行，统计各设备资源利用情况。

6.3.4. 灾备测试

城轨云平台架构设计分为主用中心和灾备中心，云测试平台验证主用中心故障后，是否具备满足业务系统应用级灾备及数据级灾备需求。

测试类别	业务系统	测试方法
------	------	------

灾备测试	ATS	灾备中心部署应用服务器、数据库服务器，应用完成数据同步及主备切换
	PIS	利用备份实现
	ISCS/AFC/ACS	应用虚拟机：利用云平台 CSDR 机制，倒切至灾备中心 数据库：灾备中心部署虚拟机，通过数据库软件实现主备中心数据库同步

6.4. 测试总结

呼和浩特城轨云测试平台测试结果表明：云平台可满足城市轨道交通业务系统需求，通过云平台资源灵活调配可提升 50%以上的硬件资源利用率，利用主用中心、站段云和灾备中心节点形成三层系统保障机制，提升城轨业务服务的可靠性，不仅给城轨云自身的兴建、运营、维护带来显著的经济效益，也为推动城轨云平台行业的信息化、智能化标准的制定及实践作出贡献。

7. 工程实施

7.1. 设备安装

7.1.1. 施工前检查

在云平台安装工程之前，必须对云平台设备间的建筑和环境条件进行检查，具备下列条件方可开工：

1. 设备间的土建工程（墙面、照明等）已全部竣工，室内墙壁已充分干燥。设备间门的高度和宽度不妨碍设备搬运，房门锁闭和钥匙齐全；
2. 设备间地面应平整光洁，预留暗管、地槽和孔洞的数量、位置尺寸应符合工艺设计要求；
3. 在铺设活动地板（静电地板）的设备间内，应对活动地板（静电地板）进行专门检查，地板板卡铺设应严密坚固，符合安装要求，地板应接地良好，接地电阻和防静电措施应符合要求；
4. 消防专业、上下水专业预留综合支吊架、管道、线缆等已安装完成，不能再进行产生灰尘、潮气等的施工作业；
5. 空调专业设备应安装完毕，性能良好，设备间的通风管道应清扫干净；
6. 供电电源已经接入设备间，综合接地箱安装完成（要求提供测试合格报告），进行位置确认及接地电阻复测；
7. 综合接地箱安装完成，进行位置确认及接地电阻复测。

7.1.2. 安装工艺

1. 微模块安装要求：
 - 地面固定稳定（螺栓齐全，紧固，承重点无悬空）；
 - 并柜连接及处理柜间缝隙；
 - 垂直度偏差不大于 3mm，两相邻机柜水平误差不大于 2mm；
 - 柜间缝隙不大于 2mm；
2. 走线架安装要求：
 - 连接完整，螺栓齐全，紧固；

- 不得闭环布置；
- 地线连接符合要求；
- 3. 布线工艺要求：
 - 布线原则
 - 路径最短，减少麻烦；
 - 走直不走弯，走弯不绕圈；
 - 进出线分开，维护查找快；
 - 绑扎适中，不伤不松；扎带剪齐，不伤手皮；
 - 弯曲圆滑饱满，不现皱褶和死弯；
 - 强弱分开，避免出怪；
 - 严禁中间接头，维护发愁；
 - 严禁绕弯打结，早晚断折。
 - 设备连线工艺要求
 - 设备/端子接线处，出线鹅头长度一致，弯曲半径一致，成型高度一致；
 - 接线链接牢固可靠，相互平行，不得歪斜；
 - 线号标识，字迹清晰，整齐美观；
 - 不得以设备端口承重线把；
 - 未使用的端口须及时设置防尘防锈封堵，做到不使用不开封，即开随封。
 - 注意事项
 - 光缆、电缆：光电成端须设置专用的光电固定装置；成端完成后须在光电规定位置设置标识牌，标识牌字迹清晰，不得手写；
 - 网线、屏蔽线、串口线（超五类、超六类线）：线缆注意屏蔽层（编织网）必须接地良好，在成端处屏蔽层剥开不得超过规定值，否则影响系统传输效果甚至引起宕机；芯线（对绞）扭绞关系，在成端处对绞关系打开长度超过规定值；在设备连接端口处连线一般预留一定长度的鹅头分枝线把不得以设备端口承重，须设置理线器或走线横梁等，避免端口插拔影响其他端口；
 - 跳线，光纤跳线：注意绑扎力度适中，弯曲不得超过允许弯曲半径，否则芯线玻璃纤维易断裂；
 - 电源线：柜内电源线布置位置要求与信号线分开，如空间限制无法分开时设置金

属槽（管）隔离。

4. 防雷与接地

● 防雷接地

- 防雷接地连线必须一点接地、星型连接，严禁多个手拉手串接；
- 连线在 0.5 米内采用线径不小于 1.5mm^2 绝缘线，连线大于 0.5 米采用线径 $2.5\sim 4\text{mm}^2$ 绝缘线；
- 防雷器件数量多而集中布置时，采用扁铜母线（镀镍）布置引接线，然后分别连接防雷器件；
- 布线最短路径，不预留，端子鹅头以 2 次做头为宜；
- 布线与电源线、信号线隔离。

● 安全接地

- 所有机柜均设置安全接地汇流排，同一排机柜共用一根接地引接线，机柜间冗余串联或根据业主业主要求设置专用接地引接线，线径不小于 16mm^2 多股绝缘阻燃软线（黄绿色）；
- 安全接地连线一般采用线径 $2.5\sim 4\text{mm}^2$ 绝缘软线；
- 柜内所有设备外壳均需与安全接地汇流排连接；
- 柜体须与安全接地汇流排连接；
- 柜门与柜体须连接接地线，上下双地线连接，采用编制铜线；
- 柜门与柜体连接地线端子设置高度一致，距离上/下门边缘为 150~200，一般为 M6 螺栓；
- 连线采用 U 形工艺，长度满足开门 180 度，确保关门不夹线。

● 屏蔽接地

- 光缆加强钢丝接地；
- 电缆金属护套及屏蔽层接地；
- 屏蔽线屏蔽层接地。

7.1.3. 施工组织

1. 按照云平台主中心、灾备中心、站段各项功能，从物理位置和设备类型上面都划分了优先级，首先确保主中心云平台机房的全功能满足需求，这是整个云平台的核心；

其次确保站段云平台的网络设备能正常安装使用，这是站段与中心联通的关键；最后确保站段及灾备中心云平台机房的条件，满足整个云平台的运行环境要求。这样划分优先级之后，就可以分清主次，按照重点依次抓，确保最关键机房的条件满足需求。

2. 主中心云平台机房是整个云平台的核心位置，无论是交付时间还是机房环境都要有严格的要求。我们在机房设计阶段就参与到方案的制定，组织云平台设计、监理、施工、厂家等单位与机房建设相关设计、施工单位对接，从机房布局、空调设置、送风方式、顶面防水、地面保温、地板高度、净空高度、机柜排布、走线方式、孔洞预留等全面沟通，确定方案，并在实施过程中严格监督，确保机房按期、保质完成交付。
3. 注意事项：
 - 1) 机房内设备安装期间存在土建单位、云平台专业、消防专业、空调专业等多家专业交叉施工问题，该期间需明确机房管理权，加强成品保护。
 - 2) 土建单位、消防专业、云平台专业等设备安装均对空间有要求，需各方设计单位、施工单位进行沟通确定，否则影响设备维修空间、空调专业下送风冷量等问题。
 - 3) 做好柜内各类型设备首件定标工作，避免大批量安装后的返工；关注异型设备安装及验收。

7.2. 系统调试

7.2.1. 测试平台

1. 搭建目的
 - 1) 对城轨云平台系统设备样机的需求符合性进行验证。
 - 2) 对城轨云平台技术及设备的测试与验证。
 - 3) 对城轨云平台全系统、全功能集成验证。
 - 4) 验证城轨云平台承载各业务系统功能、性能要求的符合性，并为安全评估与认证、上线运行提供支撑。
2. 调试阶段
 - 1) 第一阶段的调试工作为云平台功能测试，即云平台自测试；
 - 2) 第二阶段的调试工作为业务系统功能及兼容性测试，即业务系统上云后的自测试；
 - 3) 第三阶段的调试工作为容灾测试，即对业务系统和云平台故障场景下的业务倒切测试；

- 4) 第四阶段的调试工作为性能测试，即对业务系统和云平台的压力测试。

3. 测试平台实施流程

- 1) 以云平台架构为基础，提取核心设备和典型设备作为最小系统，选取功能和接口全覆盖的最大子集作为最小系统的首选模型，采用功能接口全部预留和增量式的整体架构，确定测试平台所需设备清单，并根据已确定的物理设备架构结合测试平台搭建场地实际情况规划测试平台设备板位图，规划过程中需考虑后续测试平台扩展所需物理位置预留。
- 2) 根据已确定的测试平台设备清单规划设备来源，如需借用现场设备，提前与设备厂商沟通保证供货时间并合理调配设备出处保证测试平台使用时间。
- 3) 测试平台设备到场后，为保障平台硬装及自调试工期的可控性，协调技术人员进行现场安装督导，保证布线准确性及测试平台搭建的及时性。
- 4) 测试平台搭建完成后，按照测试平台资源规划发放各业务系统对应资源，业务系统在确认资源状态后开始部署，并在部署完成后进行功能验证及兼容性测试。
- 5) 在业务系统完成上云部署后，即可开展各业务系统的容灾测试。按照招标要求对各业务系统的容灾需求编写测试用例，按照测试用例测试并做好测试记录。
- 6) 在业务系统完成上云部署后，即可开展各业务系统的性能测试，按照前期测试用例进行测试并记录测试结果，完成测试后根据测试记录产出性能测试报告。

4. 测试平台实施经验

- 1) 作为云平台集成商总包，需及时协调分包商与各上云业务厂商工作，了解各业务系统需求。
- 2) 平台搭建过程中，建议协调监理直接在测试平台开箱验货，避免后续设备验收问题。记录清楚平台使用设备（从何处借用、用到何处）以便后续归还至现场。
- 3) 做好测试平台搭建前的设计准备工作，例如：物理设备接口确认、业务系统传统部署与上云部署的风险评估与规避、关键设备数量与安装方案可行性、设备型号与正式环境的统一。
- 4) 做好测试平台及各业务系统管理工作，要求每日进出测试平台实验室进行人员登记并提交工作日报（包含当日测试内容及进度、测试问题等），并对业务系统的测试版本进行收集管控。

7.2.2. 云平台搭建

1. 搭建前检查

- 1) 设备安装准确，布线准确可用

- 2) 机房供电系统稳定
- 3) 空调已投入使用，机房温湿度适宜服务器正常运行
2. 搭建流程
- 4) 按照优先安全生产网的原则进行搭建
- 5) IT、数通现场人员分别对对应设备(服务器、交换机、防火墙)进行初始化配置
- 6) 数通现场人员进行云平台管理网搭建
- 7) IT 现场人员在云平台管理网络搭建完成后开始云平台软件（云管、虚拟化、桌面云）搭建
- 8) 云平台搭建完成后，可通过云管理平台发放云资源
3. 搭建经验
- 1) 根据现场工作量制定搭建计划，要求云平台厂家按时完成搭建任务
- 2) 搭建过程中遇到的物理链路连通性问题及时反映，要求施工方整改。

7.2.3. 业务系统资源发放

1. 上云流程
- 1) 业务系统提供提资需求表，云平台核对确认是否与设计一致
- 2) 业务系统提供上云操作系统镜像，云平台根据镜像制作对应系统模板
- 3) 根据业务系统提资表，云平台发放资源
- 4) 业务系统登陆云资源确认，并开始进行业务系统部署
2. 上云组织经验
- 1) 可在测试平台时确认各业务系统所用镜像及云平台对应系统模板，做好标记以便现场搭建直接使用
- 2) 根据各业务系统上云资源规模，合理安排对接时长
- 3) 安排各业务系统逐个与云平台对接，避免现场混乱影响施工进度。

7.3. 联合调试

7.3.1. 业务系统与云平台联调

1. 联调内容

1) 业务系统云平台资源网络互访

2) 业务系统与云平台非云对接

3) 业务系统间网络互访

2. 联调经验

1) 云平台集成商收集各业务系统内部云上、云桌面、站段后备服务器、非云间的网络互访关系，根据各业务系统间互访需求，业务系统及云平台放通相应路由，并由业务系统进行验证

2) 按照业务系统互访关系的复杂程度合理安排对接云平台顺序

3) 根据规划，云平台和业务系统各自配置非云对接交换机互联 IP 并验证非云对接状态。

7.3.2. 安全调试

1. 安全调试内容

1) 安全策略部署是云平台系统调试的最后环节，在各业务系统上云完成并且趋于稳定后，开始布置安全设备，包括以下内容：互联网出口 DDOS 设备部署、互联网出口 IPS 设备部署、WAF 设备部署、互联网出口防火墙部署、终端准入系统、日志集中管理、UMA 配置部署、漏洞扫描部署、数据审计部署、沙箱部署、态势感知部署。

2) 安全设备部署完成后会根据不同业务系统的需求，进行安全策略部署，其中调试过程中使用的路由以及不必要的业务系统互访都会进行策略收紧，仅保留生产运营所需要的策略，这是对云平台系统安全的保障。

3) 根据业务系统对其云桌面的访问需求，在云桌面管理平台制作相关网络安全组，对各业务系统云桌面进行网络隔离。

2. 安全调试经验

1) 在安全调试过程中会对无命中的策略进行删除或收紧，此操作需业务系统配合检查并持续调优，故需尽早进行。

2) 安全策略需做好备注，并在网络稳定后导出作为备份。

7.3.3. 容灾及故障测试

1. 测试内容

1) 在灾备中心云平台搭建完成后，进行云平台的容灾功能测试及业务系统的主备中心业务倒切测试

2) 在对云平台物理设备、网络配置、物理链路的故障模拟时，通过业务系统的软件状

态确定云平台的高可靠性

- 3) 在非云对接完成后，通过对非云对接主物理链路断开后业务系统至云平台的网络状态来判断非云对接的高可靠性
- 4) 在云上业务系统部署完成后，通过对业务系统两台裸金属服务器的单台故障模拟，测试业务系统单节点是否可依然正常提供服务

2. 测试经验

- 1) 云平台的可靠性需业务系统配合进行测试，故需推动业务系统配合共同测试验证
- 2) 容灾功能及故障模拟测试均为验证云平台所承载业务的可靠性，故建议在开通前完成此项测试。

7.3.4. 业务系统数据备份

1. 备份内容

- 1) 对云平台各业务系统数据库提供备份服务，并按照业务系统所需备份方式及备份周期进行备份操作
- 2) 对云平台各业务系统关键文件提供备份服务，并按照业务系统所需备份方式及备份周期进行备份操作

2. 备份经验

- 1) 因业务系统所用数据库类型及版本多样性，应在测试平台测试备份软件的可行性
- 2) 需组织业务系统进行数据恢复测试，验证所备文件或数据库的可还原
- 3) 由备份产生的归档日志可能会影响业务系统云资源的硬盘空间，需业务系统定期查看磁盘空间与日志大小，避免磁盘空间不足导致的服务异常。

7.4. 项目验收

城轨云作为城轨行业和云平台行业的结合产物，验收时应结合两方面的验收特点。具体表现为：城轨云平台为各业务系统提供计算、网络、存储、安全等基础环境，要求云平台早于业务系统具备验收条件。同时云平台虽具备独立施工条件，但云平台建成后不能独立生产或产生经济效益。因此结合以上特点，将云平台划分为一个单位工程，验收时依据单位工程验收标准进行验收。

7.4.1. 验收内容

1. 按照城轨云的物理位置、网络逻辑结构主要划分为五个分部：

- 1) 主中心云平台
- 2) 灾备中心云平台
- 3) 停车场云平台
- 4) 车辆段云平台
- 5) 车站云平台

2. 按照工程实施范围主要划分为七个分项：

- 1) 管槽安装
- 2) 线缆布放
- 3) 设备安装
- 4) 设备配线
- 5) 电源与接地
- 6) 软件安装
- 7) 功能检验。

针对城轨云工程项目的功能检验主要对机房配套动环系统、云平台系统、大数据平台系统进行验收。

1. 机房配套动环系统主要涵盖：

- 1) 智能配电柜监测
- 2) 智能 PDU 监测
- 3) 温湿度监测
- 4) 空气质量（颗粒、硫化物、烟雾）监测
- 5) 漏水监测等

2. 云平台系统主要涵盖：

- 1) 云平台运营管理
- 2) 云平台云服务
- 3) 云平台运维管理
- 4) 云平台容灾服务
- 5) 云平台网络可靠性

3. 大数据平台系统主要涵盖：

- 1) 数据采集集成
- 2) 数据存储管理
- 3) 数据分析管理
- 4) 运营信息发布管理
- 5) 生产数据分析
- 6) 智能运维管理

4. 云平台系统验收内容除去云平台系统自身部分，还应对业务系统部分内容进行验收：

- 1) 业务系统网络倒切测试
- 2) 云上业务系统的容灾测试
- 3) 业务系统备份测试。

7.4.2. 验收检查标准

7.4.2.1. 外观验收

1. 管槽安装

- 1) 布线导管或桥架的材质、性能、规格以及安装方式的选择应考虑敷设场所的温度、湿度、腐蚀性、污染以及自身耐水性、耐火性、承重、抗挠、抗冲击等因素对布线的影响，并应符合安装要求。
- 2) 缆线敷设在建筑物的吊顶内时，应采用金属导管或槽盒。
- 3) 布线导管或槽盒在穿越防火分区楼板、墙壁、天花板、隔墙等建筑构件时，其空隙或空闲的部位应按等同于建筑构件耐火等级的规定封堵。塑料导管或槽盒及附件的材质应符合相应阻燃等级的要求。
- 4) 布线导管或桥架在穿越建筑结构伸缩缝、沉降缝、抗震缝时，应采取补偿措施。
- 5) 布线导管或暗盒敷设于楼板时不应穿越机电设备基础。
- 6) 暗敷设在钢筋混凝土现浇楼板内的布线导管或槽盒最大外径宜为楼板厚的 $1/4 \sim 1/3$ 。
- 7) 建筑物室外引入管道设计应符合建筑结构地下室外墙的防水要求。引入管道应采用热浸镀锌厚壁铜管，外径 $50\text{mm} \sim 63.5\text{mm}$ 钢管的壁厚度不应小于 3mm ，外径 $76\text{mm} \sim 114\text{mm}$ 钢管的壁厚度不应小于 4mm 。

- 8) 建筑物内采用导管敷设缆线时，导管选用应符合下列规定：
- a. 线路明敷设时，应采用金属管、可挠金属电气导管保护。
 - b. 建筑物内暗敷设时，应采用金属管、可弯曲金属电气导管等保护。
 - c. 导管在地下室各层楼板或潮湿场所敷设时，不应采用壁厚小于 2.0mm 的热镀锌钢管或重型包塑可弯曲金属导管。
 - d. 导管在二层底板及以上各层钢筋混凝土楼板和墙体内敷设时，可采用壁厚不小于 1.5mm 的热镀锌钢导管或可弯曲金属导管。
 - e. 在多层建筑砖墙或混凝土墙内竖向暗敷导管时，导管外径不应大于 50mm。
 - f. 由楼层水平金属槽盒引入每个用户单元信息配线箱或过路箱的导管，宜采用外径 20mm~25mm 钢导管。
 - g. 楼层弱电间（电信间）或弱电竖井内钢筋混凝土楼板上，应按竖向导管的根数及规格预留楼板孔洞或预埋外径不小于 89mm 的竖向金属套管群。
 - h. 导管的连接宜采用专用附件。
- 9) 槽盒的直线连接、转角、分支及终端处宜采用专用附件连接。
- 10) 在明装槽盒的路由中设置吊架或支架，宜设置在下列位置：
- a. 直线段不大于 3m 及接头处；
 - b. 首尾端及进出接线盒 0.5m 处；
 - c. 转角处。
- 11) 布线路由中每根暗管的转弯角不应多于 2 个，且弯曲角度应大于 90°。
- 12) 过线盒宜设置于导管或槽盒的直线部分，并且设置在下列位置：
- a. 槽盒或导管的直线路由每 30m 处；
 - b. 有 1 个转弯，导管长度大于 20m 时；
 - c. 有 2 个转弯，导管长度不超过 15m 时；
 - d. 路由中有反向（U 形）弯曲的位置。
- 13) 导管管口伸出地面部分应为 25mm ~ 50mm。

2. 线缆布放

- 1) 建筑物内缆线的敷设方式应根据建筑物构造、环境特征、使用要求、需求分布以及所选用导体与缆线的类型、外形尺寸及结构等因素综合确定，并应符合下列规定：

- ① 水平缆线敷设时，应采用导管、桥架的方式，并应符合下列规定：

- a. 从槽盆、托盘引出至信息插座，可采用金属导管敷设；
- b. 吊顶内宜采用金属托盘、槽盒的方式敷设；
- c. 吊顶或地板下缆线引入至办公家具桌面宜采用垂直槽盒方式及利用家具内管槽敷设；
- d. 墙体内应采用穿导管方式敷设；
- e. 大开间地面布放缆线时，根据环境条件宜选用架空地板下或网络地板内的托盘、槽盒方式敷设。

② 干线子系统垂直通道宜选用穿楼板电缆孔、导管或桥架、电缆竖井三种方式敷设。

- 2) 建筑群之间的缆线宜采用地下管道或电缆沟方式敷设。
- 3) 明散缆线应符合室内或室外敷设场所环境特征要求，并应符合下列规定：
 - a. 采用线卡沿墙体、顶棚、建筑物构件表面或家具上直接敷设，固定间距不宜大于 1m。
 - b. 缆线不应直接敷设于建筑物的顶棚内、顶棚抹灰层、墙体保温层及装饰板内。
 - c. 明敷缆线与其他管线交叉贴邻时，应按防护要求采取保护隔离措施。
 - d. 敷设在易受机械损伤的场所时，应采用铜管保护。

3. 设备安装

- 1) 综合布线系统宜采用标准 19" 机柜，安装应符合下列规定：
 - a. 机柜数量规划应计算配线设备、网络设备、电源设备及理线等设施的占用空间，并考虑设备安装空间冗余和散热需要。
 - b. 机柜单排安装时，前面净空不应小于 1000mm，后面及机列侧面空不应小于 800mm；多排安装时列间距不应小于 1200mm。
- 2) 在公共场所安装配线箱时，暗装箱体底边距地面不宜小于 1.5m，明装式箱体底而距地面不宜小于 1.8m。
- 3) 机柜、机架、配线箱等设备的安装宜采用螺栓固定。在抗震设防地区，设备安装应采取减震措施，并应进行基础抗震加固。

4. 电源与接地

- 1) 综合布线电缆与附近可能产生高电平电磁干扰的电动机、电力变压器、射频应用设备等电器设备之间应保持间距，与电力电缆的间距应符合下图标准：

类别	与综合布线接近状况	最小间距
380V 电力电缆	与缆线平行敷设	130

< 2kV.A	有一方在接地的金属槽盒或钢管中	70
	双方都在接地的金属槽盒或钢管中	10
380V 电力电缆 2kV.A ~ 5kV.A	与缆线平行敷设	300
	有一方在接地的金属槽盒或钢管中	150
	双方都在接地的金属槽盒或钢管中	80
380V 电力电缆 > 5kV.A	与缆线平行敷设	600
	有一方在接地的金属槽盒或钢管中	300
	双方都在接地的金属槽盒或钢管中	150

2) 室外墙上敷设的综合布线管线与其他管线的间距应符合下图标准:

其它管线	最小平行净距	最小垂直交叉净距
防雷专设引下线	1000	300
保护地线	50	20
给水线	150	20
压缩空气管	150	20
热力管 (不包封)	500	500
热力管 (包封)	300	300
燃气管	300	20

- 3) 综合布线系统应远离高温和电磁干扰的场地, 根据环境条件选用相应的缆线和配线设备或采取防护措施, 并应符合下列规定:
 - a. 当综合布线区域内存在的电磁干扰场强低于 3V/m 时, 宜采用非屏蔽电缆和非屏蔽配线设备。
 - b. 当综合布线区域内存在的电磁干扰场强高于 3V/m, 或用户对电磁兼容性有较高要求时, 可采用屏蔽布线系统和光缆布线系统。
 - c. 当综合布线路由上存在干扰源, 且不能满足最小净距要求时, 宜采用金属导管和金属榄盒敷设, 或采用屏蔽布线系统及光缆布线系统。
 - d. 当局部地段与电力线或其他管线接近, 或接近电动机、电力变压器等干扰源, 且不能满足最小净距要求时, 可采用金属导管或金属槽盒等局部措施加以屏蔽处理。
- 4) 在建筑物电信间、设备间、进线间及各楼层信息通信竖井内均应设置局部等电位联结端子板。

- 5) 综合布线系统应采用建筑物共用接地的接地系统。当必须单独设置系统接地体时，其接地电阻不应大于 4Ω 。当布线系统的接地系统中存在两个不同的接地体时，其接地电位差不应大于 $1V_{r.m.s.}$ 。
- 6) 配线柜接地端子板应采用两根不等长度，且截面不小于 $6mm^2$ 的绝缘铜导线接至就近的等电位联结端子板。
- 7) 屏蔽布线系统的屏蔽层应保持可靠连接、全程屏蔽，在屏蔽配线设备安装的位置应就近与等电位联结端子板可靠连接。
- 8) 综合布线的电缆采用金属管槽敷设时，管槽应保持连续的电气连接，并应有不少于两点的良好接地。
- 9) 当缆线从建筑物外引入建筑物时，电缆、光缆的金属护套或金属构件应在入口处就近与等电位联结端子板连接。
- 10) 当电缆从建筑物外面进入建筑物时，应选用适配的信号线路浪涌保护器。

7.4.2.2. 功能验收

功能组验收部分参考 IT 行业的验收内容和标准，同时加入业务系统需要的基本功能，控制中心内测试 32 项内容，车站内测试 9 项内容，动环系统测试 4 项内容，数据挖掘测试 29 项内容。

生产中心验收测试内容：

序号	验收测试内容	序号	验收测试内容	序号	验收测试内容
1	VDC管理	12	租户资源监控	23	虚拟机桌面基本业务
2	配额管理	13	集中告警	24	虚拟桌面业务管理
3	产品管理	14	单点登录	25	虚拟桌面基础安全
4	计量计费	15	防火墙服务	26	远程重启虚拟桌面
5	VDC自运维	16	裸金属服务	27	客户端资源映射
6	基础网络服务	17	云硬盘高可用服务	28	网络设备远程登录
7	弹性云服务器 (KVM)	18	云服务器容灾服务	29	网络设备软件版本查看
8	镜像服务 (Swift)	19	计算虚拟化	30	网络设备硬件信息查看
9	云硬盘服务	20	网络虚拟化	31	网络设备网络配置信息查看
10	系统资源监控	21	存储虚拟化	32	网络可靠性测试
11	容量管理	22	集成管理业务		

车站验收测试内容：

序号	验收测试内容	序号	验收测试内容	序号	验收测试内容
1	计算虚拟化	4	集成管理业务	7	网络设备硬件信息查看
2	网络虚拟化	5	网络设备远程登录	8	网络设备网络配置信息查看
3	快照与数据恢复	6	网络设备软件版本查看	9	网络可靠性功能

动环系统验收测试内容：

序号	测试内容	序号	测试内容
1	动环软件显示数据与现场数据的一致性	3	动环本地监控
2	动环软件显示告警的一致性、时效性	4	门禁管理

数据挖掘验收测试内容：

序号	测试内容	序号	测试内容
1	数据挖掘平台提供对异构数据源的集成能力，根据各类数据资源采用不同的采集策略，实现多种数据处理技术框架。	16	对设备监视数据进行分析，统计故障情况，同时对设备使用次数进行统计
2	数据挖掘平台提供混合存储能力，按照预定的采集策略对不同数据类型分别存储，同时支持建模功能和多维度高速查询。	17	对以上故障数据进行分析，提供维修建议
3	作为数据挖掘平台的用户接口为使用者提供统一的作业调度工具，提供可视化ETL作业、报表作业、分布式计算作业的自动调度平台，提供作业之间的依赖管理和作业的监控管理。	18	对客流数据进行分析，包括进出站量、换乘客流、断面客流、拥挤度
4	运营决策支持管理，按照系统级、线路级、部门层级等设计管理场景，将指标进行图形/报表展示。	19	建立拥挤度的颜色判别原则，制定客流密度指标，对不同维度的客流量进行预测。
5	对不同主题的数据进行采集，实现系统采集和人工填报两种方式。	20	对票/数据进行分析，通过闸机交易数据对票卡数量、类型、金额进行统计，同时对票/款管理信息进行统计
6	数据可实现日、周、月的自动统计，以报告形式呈现	21	进行生产调度管理，接收不同渠道的设备故障情况并派发工单，对维修记录进行管理和统计分析
7	实现对用户的管理，根据不同层级设置不同的权限，系统管理员可对用户进行增删改查操作。	22	实现现场维修管理，包括签到签退、任务交接、设备扫码等功能
8	实现用户角色组的配置	23	实现设备履历管理，管理设备基础信息和设备的故障处理、检修记录。
9	对ATS子系统数据进行分析，包括运行状态数据、运行数据、列车服务质量等。	24	对列车运营指标进行统计
10	对转辙机工作数据进行分析，包括对道岔动作时间、动作电流、缺口超限的统计和对一启动继电器、定反操继电器、表示继电器的数据分析。	25	对转辙机故障状态进行监视
11	对信号车载数据进行分析，包括ATO停车精度数据以及对雷达、速度传感器故障进行统计分析	26	对车载测速系统状态进行监测
12	对车地通信质量进行分析，包括场强异常值的统计分析	27	对车地通信质量进行监测
13	对终端设备功能质量进行分析，包括对工控机/服务器的工作时间、温度、硬盘占有率、CPU占有率的监控	28	对车载ATPATO故障进行监测
14	对以上故障数据进行分析，提供维修建议	29	对CI设备故障进行检测
15	对模式管理数据进行分析，当监测到出发紧急模式时发出报警		

7.5. 典型问题

7.5.1. 设计阶段

现场施工作业中，机房内工作面应尽量由一方全部负责，保证机房内工艺统一、美观。如必须划分作业面，则要考虑现场实际情况，保证施工的交叉面尽可能少，减少不同的作业面交叉带来工艺上的冲突。

企业信息管理网中的办公云桌面所需的操作系统、防病毒软件、办公软件供应方应明确，否则会出现办公系统功能、安全等方面的问题，明确供应方后，各自负责相应的界面，保证办公系统的功能及安全。

由于云平台至互联网出口链路与企业内网为同一链路，导致内网用户使用企业网 WIFI 通过手机 APP 访问云平台业务时需额外进行策略路由匹配，导致某些场景下访问不便。建议云平台至互联网出口链路与企业内网独立设置。

在设计阶段应考虑云平台与业务系统间的设备接口，尽量采用光纤对接，避免因网线传输距离受限，添加光纤转换器，影响机柜内设备布局的规范和美观。

7.5.2. 测试平台测试阶段

搭建测试平台，应考虑测试平台的设备来源，如果为测试平台单独采购设备，平台可进行充分测试。如果从现场的设备中进行借用，需考虑现场工期与测试平台工期的冲突，应尽量提前测试平台的开始时间，防止影响现场的工期。

测试平台及各业务系统管理，目前呼和浩特云测试平台要求各业务系统进出实验室登记，每天提交日报，包含当日测试内容及进度，测试问题等，并对业务系统测试版本进行收集管控。

7.5.3. 设备安装阶段

在设备进场安装前应保证数据机房安装环境具备条件，包括照明正常、防静电施工完成、温湿度在正常范围内、远离污染物（灰尘、腐蚀性气体等）等以保证设备上电后的正常运行。

数据机房设备所配备的接地线应满足当前机柜接地铜排、机房接地母排等所采用的接地方式，以保证设备接地正常，满足设备正常运行。

设备布线应按照相关标准及工艺，且需考虑具体设备位置，设备通信光电缆与电源线走线位置，按照实际情况配备光电缆的规格。

在设计阶段应充分考虑核心交换机等异型设备规格大小造成的机柜适配性，保证机柜既可满足异性设备安装又满足柜内气流走向。

7.5.4. 系统调试阶段

业务系统在启动网络设备前需与云平台网络技术人员进行可行性分析，在确认对现有网络无影响后方可开启设备，如无法确认对现有网络是否存在影响，在向调度申请施工窗口后再开启设备。

在联调期间，施工布线等存在影响业务系统使用的施工作业，需提前通知相关业务系统协调时间，并在前期施工对已承载业务的线缆做好标签（至少有临时标签）。

- 1) 建设单位应在做涉及影响云平台机房电力的操作时提前和我方取得联系，确保我方做好设备下电后再施工。
- 2) 网络设备在每次做完配置更改后做好保存工作。
- 3) 确保平台恢复顺序为：网络恢复、存储恢复、服务器恢复。

由于平台承载业务较多且告警信息类型复杂，应区别报警声音，方便运营人员通过声音区别问题的紧急程度，从而做出相应措施。

7.5.5. 联合调试阶段

业务系统与云平台对接时，出现业务侧为赶进度，以简化组网进行对接，与预期结果不一致，导致二次对接。建议业务系统与云平台联调时按照约定的接口方式对接，避免返工。

多业务间调试时，容易出现对接方式、数据格式等不一致，或临时调整现象，导致云平台侧多次调整网络配置及安全策略。建议云平台作为集成方协调各业务系统，梳理业务间互访关系，明确边界与接口。

多业务调试时，由于双方调试信息不同步，双方各自操作造成互相影响，建议业务调试时涉及接口部分，应及时告知对方专业，缩小调试干扰变量。

涉及网络接口调试时，其他设备商出现业务交换机配置未保存，当设备下电或重启时配置丢失，造成返工。

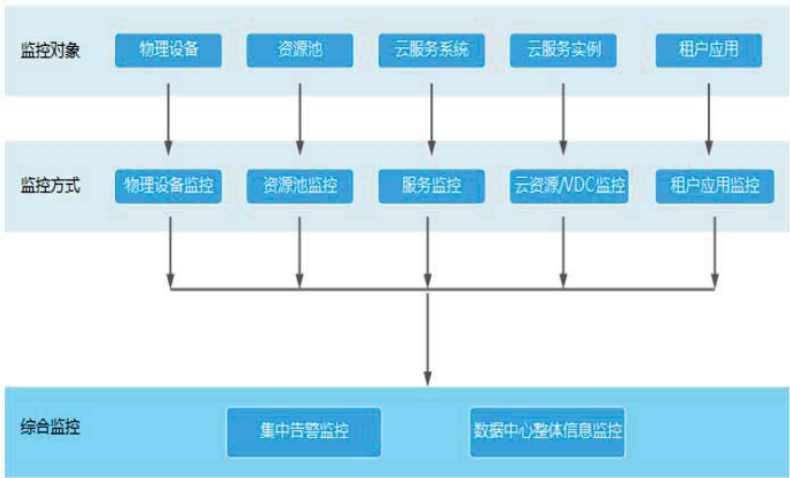
8. 城轨云运维

8.1. 日常运维

云平台的维护工作主要是平台状态管理、资源管理、例行检查、预案管理及数据备份。

1. 平台状态管理

运维人员通过运维平台的统一告警及进入机房的例行巡检两部分工作的结合来实现对整网的资源、告警、性能、容量使用情况进行监控，实时了解网元以及 IT 资源的健康状态。



立体化全景监控包括对象监控和综合监控：

1) 对象监控：

- a. 物理设备监控：服务器设备、网络设备、存储设备的告警、拓扑、性能等监控。
- b. 资源池监控：计算资源、存储资源、网络资源的容量、性能、负载等监控。
- c. 服务监控：云管理系统服务以及云服务系统运行的告警、性能等监控。
- d. 云资源/VDC 监控：云资源和 VDC 视角下，资源实例（计算、存储、网络、安全等）的告警、性能等监控。
- e. 租户应用监控：基于应用的资源统计和监控。

2) 综合监控：

- a. 集中告警监控：系统服务或第三方系统告警的集中监控。
- b. 数据中心整体信息监控：对不同区域数据中心的资源、告警、容量等维度的数据进行统计，通过不同的 Dashboard 页面直观地展示数据中心的整体运行状况

2. 资源管理

运维人员还需梳理各云上业务系统云服务器资源状况、数据分布情况、网络专线及带宽情况。根据对业务系统资源实际使用情况的长期统计与观察，提出合理的资源规格建议，确保云平台资源的充分利用。

3. 例行检查

制定服务例行排查点，并不断完善。根据制定的服务排查点，对服务进行定期检查。对排查过程中发现的问题，及时进行追查，排除可能存在的隐患。

4. 预案管理

确定所需的各项监控、系统指标的阈值或临界点，以及出现该情况后的处理预案。建立和更新服务预案文档，并根据日常故障情况不断补充完善，提高预案完备性。能够制定和评审各类预案，周期性进行预案演练，确保预案的可执行性。

5. 数据备份

制定数据备份策略，按规范进行数据备份工作。保证数据备份的可用性和完整性，定期开展数据恢复性测试。

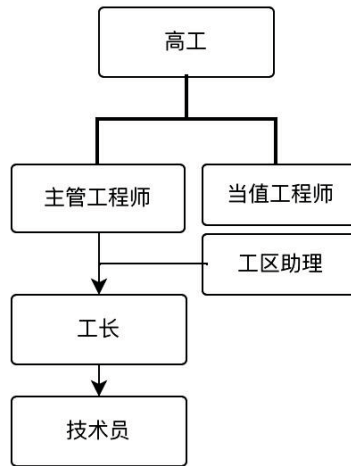
8.2. 安全防护

云平台的安全防护运维主要是指负责云平台网络、系统和业务等方面的安全加固工作，进行常规的安全扫描、渗透测试，进行安全工具和系统研发以及安全事件应急处理。防护工作包括：

1. 安全制度建立：根据内部的具体流程，制定切实可行，且行之有效的安全制度。
2. 安全培训：定期向使用方提供具有针对性的安全培训和考核，建立安全负责人制度。
3. 风险评估：通过定期对云平台整体进行巡检，产出对物理网络、服务器、业务应用、用户数据等方面的总体风险评估结果。
4. 安全建设：根据风险评估结果，加固薄弱环节，包括对高危端口的禁用、设备更新补丁、病毒库升级等手段做好云平台安全建设工作。

8.3. 运维架构

根据呼和浩特城轨云平台规模、设备数量、设备分布，运维主要人员岗位结构图和职责如下：



高级工程师：

1. 编制维修管理规则，人员调配及考核
2. 关键设备的检查，设备维修质量的改善
3. 影响运行设备故障的跟进、技术报告的审核
4. 作业指导书，处置方案的组织编写、审核、修订
5. 与公司各专业/部门对接工作
6. 负责维修物资管理
7. 部门所有应急故障抢修及抢修管理
8. 部门文本及信息化软件填写及使用管理
9. 筹备期与开通前期承担与运营相关专业的指标对接及其他相关接口工作

主管工程师：

1. 工区人员的工时、考勤安排，工区人员维修质量监督及改善
2. 工区资产管理，工区维修物资管理
3. 工区简报及技术编写、更新、对外发送与措施跟进
4. 设备 PM 作业指导书的编写及验证，工区 PM 计划申报、实施
5. 工区人事及设备安全管理，工区人员及设备安全管理
6. 工区文本及电子信息软件填写、使用管理
7. 工区所有故障的跟踪
8. 接口专业协调工作

9. 工区内部业务培训工作

当值工程师

1. 故障报告的编写、更新、对外发送
2. 工区所有故障的处理、简报编写、更新、对外发送
3. 应急故障处理、抢修、组织
4. 重大预防修的指导、组织
5. 接口专业协调工作

工长：

1. 负责当班期间班组人员考勤、行为管理工作
2. 负责当班期间所有故障的处理、跟进、上报工作
3. 负责当班期间巡检、设备维护工作
4. 负责当班期间日报、DMS、UR、企业微信等信息化软件及纸质版表单的填写、审核、申报、存档工作
5. 负责当班期间班组文件学习工作
6. 负责当班期间各类处置方案应急预案演练及演练报告书写工作
7. 负责当班期间工区工具、物料、备件的使用管理工作
8. 负责组织班组人员技术学习，完成培训计划内的学习任务
9. 负责当班期间辖区各站工作

技术员：

1. 执行当班期间故障处理、跟进、上报工作；
2. 执行当班期间巡检、设备维护工作
3. 执行当班期间信息化软件及纸质版表单的填写、存档工作
4. 完成当班期间个人文件学习工作
5. 参加当班期间各类处置方案应急预案演练工作
6. 完成当班期间工区工具、物料、备件使用后的文本填写及整理工作
7. 参加班组技术学习，完成个人培训计划内的学习任务
8. 执行当班期间各站整理等工作

工区助理：

1. 配合班组应急故障抢修工作
2. 在班组人员不齐整情况下进行补班工作
3. 负责工区安全类工作，包括应急物资、劳保用品及相关材料申请、出入库、盘点、文件整理、台账更新、报审、存档工作
4. 负责工区工器具申请、出入库、盘点、送检、文件整理、台账更新、报审、存档工作
5. 负责工区备品备件、物料、办公用品申请、出入库、盘点、文件整理、台账更新、报审、存档工作
6. 负责工区人员考勤相关统计、更新、报审、存档工作
7. 负责工区各类纸质版文件及工单二次审核、台账更新、报审、存档工作
8. 负责协助工程师管理的工区各项工作。

8.4. 应急演练

运维人员需定期对云平台进行故障演练，以保证在紧急情况下做出快速响应，减少业务系统故障时间。

应急演练内容主要为：

一、容灾倒切；

场景：主用中心与车站网络通讯异常，灾备中心仍可与车站正常通讯。

建议措施：

- 1、将云平台切换为灾备中心模式。
- 2、业务系统将车站业务与灾备中心云服务器建立连接，恢复业务状态正常。

二、各业务系统切为站控模式；

场景：主用中心与灾备中心均与车站网络异常。

建议措施：业务系统将车站业务连接至车站后被服务器，恢复站内控制。

三、外界环境灾害应急；

场景：云平台设备所在房间发生火灾或温湿度异常。

建议措施：定期进行消防演练、漏水演练，确保每个运维人员清晰应急流程，掌握应急操作。

四、电力异常应急。

场景：云平台设备异常掉电。

建议措施：根据具体设备的影响业务范围，做出对应降级或应急措施。

五、设备异常应急。

场景：云平台设备状态异常，无法正常承载业务。

建议措施：导入设备配置并导入同型号备品备件中，将设备替换为备品备件设备，业务恢复。

9. 呼和浩特城轨云建设实践

呼和浩特城轨云平台系统作为国内首个多线路、多业务“城轨云”，经历三年多的努力最终完成了项目的建设落地工作。2016年4月，呼和浩特市提出并开始践行“云计算+城轨”的发展理念，用云计算、大数据技术为城市轨道交通提供地铁运营生产、企业管理、建设管理、运营管理以及资源管理等服务。之后的几年内，经过多部门联合操作，此理念率先运用到呼和浩特地铁建设中，并组织方案论证、科研立项、苏州测试研究、招投标及合同谈判、设计联络及四次云平台专家评审会、和林测试平台、城轨云创新发展与实践应用研讨会、云平台安装调试、联合调试、工程验收应用等工作，对云平台建设方案及阶段性成果展开评审。最终确定呼和浩特“城轨云”解决方案是基于“用云计算、大数据技术为城市轨道交通提供地铁运营生产、企业管理、建设管理、运营管理以及资源管理等服务”的理念，为城市轨道交通从设计、建设、运营全环节搭建智慧云平台，实现信息化业务全覆盖及统一运维管理、安全管控。

从2016年4月提出理念至今，呼和浩特市城市轨道交通建设管理有限责任公司（下称“呼和浩特市轨道交通公司”）按照“大胆设想、小心求证、测试先行、确保可靠”的原则，将科技创新“保安全、要效益、提效率”的理念贯穿地铁1、2号线一期工程建设始终。

9.1. 顶层设计

呼和浩特市轨道交通公司在管理创新过程中，始终践行“做行动的巨人，不做语言的矮子”。在实现云端生产、办公过程中，在国内率先引入了城轨云的概念。

管理创新，以云计算、大数据实现城轨云信息化，以城轨云信息化辅助实现管理智慧化。国内城轨行业无融合运用运营生产与企业管理信息化的智慧化管理先例，更无云计算统一构建生产与企业管理信息化平台的研究。为充分验证管理创新中顶层设计的合理性和可行性，验证是否可实现“一云全覆盖”的可落地性，呼和浩特市轨道交通公司以科研测试，验证顶层设计的合理性，验证智慧管理的可行性，以科学的、真实的数据，向城轨行业证明智慧管理是可行的、必要的。

呼和浩特市轨道交通公司于2016年提出了城轨云建设目标。为顺利完成项目设计和建设，决定以科研项目支撑设计、建设，开始了公司内部论证和相关调研工作。在充分调研与论证基础上，形成大量的资料和素材积淀。

2017年2月，呼和浩特城轨云应用专家研讨会召开。此次会议邀请来自北京、深圳、武汉、广州等地的建设单位、设计单位的专家，针对轨道交通行业运用云计算技术的可行性进行了深入探讨。与会专家一致认为，城轨云建设是可行的，同时具有一定前瞻性和经济社会效益，建议以科研项目的形式进行进一步验证，同时为项目设计和建设提供必要性的数据支撑。

由此，呼和浩特市轨道交通公司开展了一系列的科研立项筹备工作，并于 2017 年 3 月召开了“呼和浩特城轨云应用研究科研项目”立项专家评审会。会上专家一致认为城轨云科研立项是可行的、必要的，可以对后期的设计、建设提供必要的数据支撑。

9.2. 方案论证

城轨领域业务系统深度融合，精细化运营逐步成为行业发展趋势，而支持集中部署，运营大数据分析的业务系统云化部署将成为新的行业热点。

呼和浩特城轨云应用专家研讨会的与会专家提出测试的必要性，呼和浩特市轨道交通公司选择城轨行业业务系统主流厂家 3 至 4 个，由各厂家推选出牵头单位（如，云平台厂家华为、信号厂家交控科技、综合监控厂家和利时、通信厂家烽火科技、AFC 厂家浙大网新等），多厂家在华为苏州 OpenLab 实验室展开云平台与业务系统的兼容性等相关内容测试工作。以此为背景，呼和浩特市轨道交通公司开展了呼和浩特市城市轨道交通云平台方案的研究测试工作，旨在研究通过统一的云计算融合 IT 基础架构平台实现城轨综合监控系统（ISCS）、视频监控系统（CCTV）、自动售检票系统（AFC）、乘客信息系统（PIS）、门禁系统（ACS）、列车自动监控系统（ATS）、公专电话等业务系统的综合部署承载，最终通过资源池的平滑扩充建成统一的呼和浩特城轨云平台，实现城轨 IT 资源的供应模式由传统竖井式转变为资源共享的 IT 云服务方式。

2017 年 2 月 16 日，在呼和浩特市，呼和浩特市轨道交通公司组织召开了“呼和浩特市城市轨道交通融合云平台应用研究”科研项目建议书专家评审会和呼和浩特市城市轨道交通 1 号线一期工程融合云平台应用专家研讨会。邀请了全国主要地铁公司、设计单位等的专家对该构想进行初步评审，专家组一致认为轨道交通融合云平台科研项目具有一定技术前瞻性，具有较好的技术经济效益和推广应用前景。

2017 年 3 月 17 日，在呼和浩特市，呼和浩特市轨道交通公司组织召开了“呼和浩特市城市轨道交通融合云平台应用研究”项目进行了初步审查，专家组认为本项目研究内容及测试方案基本全面，测试方案基本可行，符合呼和浩特轨道交通建设及运营需求，将对设备招标及项目实施工作具有指导意义。

2017 年 4 月 17-28 日、5 月 7-20 日，在苏州，呼和浩特市轨道交通公司组织在苏州华为 openlab 实验室开展了第一阶段的一、二批测试，分别有 ISCS、CCTV、PIS、AFC、ACS、ATS 六个业务系统，每个业务系统各有两个厂家参加。

2017 年 6 月 21 日，在天津，呼和浩特市轨道交通公司赴中国铁设，听取了对呼和浩特市城市轨道交通线网云平台项目的整体筹划建议，正式明确了呼和浩特地铁线网级云平台的用户需求，提出建设城轨云的初步设想。

2017 年 7 月 21 日，在呼和浩特市，呼和浩特市轨道交通公司组织召开了呼和浩特城轨云平台总体技术方案专家评审会，专家组听取了中国铁设对呼和浩特城轨云平台总体技术方案的详细汇报，专家组一致认为呼和浩特城轨云平台总体技术方案内容全面，方案可行。

2017年7月22日至8月31日，在呼和浩特，呼和浩特市轨道交通公司组织，中国铁设牵头组织相关业务厂家进行了多次详细技术方案和第二阶段线网级测试方案的研讨会，制定了初步技术方案和第二阶段的线网测试方案。

2017年9月1日至11月15日，呼和浩特市轨道交通公司先后组织ISCS、CCTV、PIS、AFC、ACS、ATS、公专电话等7个业务系统厂家和华为公司，共计29个厂家，在苏州华为Open Lab实验室开展第二阶段测试，本阶段测试按照业务系统先后分了4个批次进行，以及还包括后期个别业务系统补测工作。

2017年11月1日至12月10日，针对第二阶段测试结果进行梳理和总结，中国铁设多次组织ISCS、CCTV、PIS、AFC、ACS、ATS、公专电话、华为等设备厂家进行第二阶段测试报告编写工作。

2017年11月1日至2018年1月30日，为验证各业务系统应用优化后上云部署的长期运行稳定性，呼和浩特市轨道交通公司组织各主要牵头厂家在华为苏州实验室开展了长稳测试，测试周期为3个月。

2017年12月14日，在呼和浩特市，呼和浩特市轨道交通公司组织召开了呼和浩特城轨云平台测试报告的专家评审会。

通过呼和浩特城轨云平台第一阶段测试已初步证明：按照传统架构模式构建，综合监控系统（ISCS）、自动售检票系统（AFC）、视频监控系统（CCTV）、乘客信息系统（PIS）、门禁系统（ACS）、列车自动监视系统（ATS）等基于云平台部署基本可行，云化部署后各业务系统基本功能正常，综合监控系统与其他系统间接口功能正常，云计算基础平台基本满足了各业务系统性能、可靠性等方面的需求。

呼和浩特城轨云平台第二阶段测试侧重于各业务系统云化部署后架构优化、不同厂家的异构测试验证，对各业务系统基于桌面云部署的外设兼容性，各业务系统同构&异构的性能，各业务系统优化架构下长期稳定性证、以及云平台对各业务系统的安全防护特性均进行了更为详尽的测试验证。

第二阶段测试结果：

业务系统侧：ISCS、AFC、PIS、ACS、CCTV等专业经多厂家联合验证了系统架构优化、线网级部署方案是可行的。基于线网方案可实现线网级平台与线路异构系统的互通与对接；通过云平台的安全措施及策略可保障业务系统的安全性。

云平台侧：基本功能特性如云管运营、桌面云、网络、安全防护、云管运维等基本功能验证项全部通过，基于云平台可满足各业务系统的正常云化部署实施，并满足各业务系统的网络承载与安全防护的基本需求。

2018年3月27日，由城市轨道交通列车通信与运行控制国家工程实验室、呼和浩特市轨道交通公司主办，中国铁设承办的呼和浩特市城轨云科研测试技术白皮书专家评审会在呼和浩特市顺利召开。2018年4月，《城轨云运营生产系统测试报告白皮书》由城市轨道交通列车

通信与运行控制国家工程实验室正式发布。

9.3. 科研立项

2015 年 4 月 15 日，经国务院批准，国家发改委批复呼和浩特市轨道交通首期建设规划立项。

2015 年 9 月，轨道交通 1、2 号线一期工程可行性研究报告获自治区发改委批复。

2016 年 3 月，轨道交通 1、2 号线一期工程初步设计获得市城建委批复；同年，轨道交通 1、2 号线一期工程开工。呼和浩特市城市轨道交通的批复开工，正值国内云计算大数据发展黄金期，全国各地也在积极探索基于云平台的城市轨道交通信息化建设之路，呼和浩特市充分发挥新线城市后发优势，深入贯彻党的十九大关于建设“交通强国”战略部署以及市政府打造宜居的现代化首府城市的要求，秉承建设绿色地铁、人文地铁、智慧地铁的先进理念，经过三年多创新探索，探索建设线网级城市轨道交通云平台系统，走出一条“科研-测试-工程实施-优化运营管理”的务实创新之路。

2017 年 3 月 17 日，城市轨道交通融合云平台应用科研项目通过专家评审；2017 年 9 月，完成呼和浩特市 2018 年重大科技专项项目申报；2018 年 6 月，通过呼和浩特市 2018 年重大科技专项项目答辩、现场调研；2018 年 10 月，获呼和浩特市 2018 年重大科技专项项目立项批复；2020 年 7 月，完成市重大专项科研各项任务指标，正式进入验收阶段。此外该项目入选《工业和信息化部 2019-2020 年度物联网关键技术与平台创新类、集成创新与融合应用类示范项目》。

9.4. 工程落地

在整个呼和浩特市城轨云平台的建设管理过程中，呼和浩特市轨道交通公司始终秉承“安全第一、质量保证、事争一流、唯旗是夺”的理念，全面、深入地参与到项目的建设管理过程中。不仅履行了甲方的建设管理职责，还深入到设计管理、监理管理、集成管理、施工管理的具体环节中，与各参建单位共同研究、共同推进，有力协调各相关资源，全力推进项目的落地实施，确保了国内首个线网级、多业务城轨云平台按期、高质量落地呼和浩特。

9.4.1. 实施历程

基于前期方案研究论证及测试，2018 年 4 月基本确定了呼和浩特市城市轨道交通云平台的方案和架构，呼和浩特市城市轨道交通云平台承载 1、2 号线列车自动监控系统（ATS）、综合监控系统（ISCS）、乘客信息系统（PIS）、自动售检票系统（AFC）、门禁系统（ACS）、公务电话系统（PBE）、集中告警系统（TEL/ALM）7 个生产系统，以及企业管理信息系统、乘客管理服务系统，为其提供计算资源、存储资源、网络资源等，实现基于 IaaS 层的云平台部署。

确定方案后，便展开云平台招标用户需求书的编写。编写过程中，组织公司内各部门评审，并邀请行业内专家进行为期一个多月的专项审查，分别从系统方案、系统功能、系统容量、系统安全，以及系统概算五个方面进行质询讨论、探索研究，全面完善用户需求书内容，确保了需求书的编制质量，合理、有效降低了系统投资，为云平台项目落地迈出了关键的一步。经过初稿、修正稿、会审稿各个版本的不断完善，最终于 2018 年 9 月完成了招标文件技术要求的编制工作。

呼和浩特城轨云平台按照线网级架构规划，在招标时 1、2 号线建管公司经沟通达成一致，采取委托招标的形式，确保共同打造一个线网级云平台。由于线网级、多业务的城轨云平台招标在国内尚属首次、并无先例，只有摸索最合理的招标方式才能顺利开展工作，保证招标工作既要满足需求、又能落地实施，还必须合法合规。呼和浩特城轨云平台专业招标较晚，主要业务系统招标工作均已经完成，所以城轨云平台采取了独立招标的方式，要求在城轨交通行业承担过城轨云平台承载的、具有一定规模的主要业务系统项目实施经验的单位参与，以此确保城轨云平台系统集成商的能力和水平。

2018 年 12 月 14 日，顺利完成呼和浩特城轨云平台的招标工作，12 月 24 日至 26 日，完成城轨云平台合同谈判，2019 年 1 月 7 日，召开第一次设计联络会。2019 年 1 月至 4 月期间，建设单位组织运营单位、设计单位、监理单位、施工单位、各业务系统及分包商共召开三次设计联络会，对云平台的技术问题、施工问题、项目管理问题以及云平台与各业务系统接口关系进行了梳理和优化，共计形成会议纪要 10 余份、云平台接口说明书 34 份、设计方案 2 份、详细设计说明书 11 份，经过与会各方多轮讨论，达成一致且明确的设计原则和功能要求。在设计联络期间，针对明确的需求和功能要求，陆续展开设备、机柜等的工厂生产，2019 年 3 月下旬，监理单位组织建设单位、运营单位、设计单位等进行云平台出厂验收，共同监督检查供货单位的生产质量，确保满足合同要求。

各系统供货商严格按照出厂验收提出的整改意见完成整改之后，便组织批量生产，陆续供货。2019 年 5 月部分设备开始到货，陆续开始车站云平台设备的安装，同步开展和林测试平台的搭建。经过组织云平台设计单位、施工单位、集成商、监理单位和机电安装、装修单位多次对接，协调各方安装接口与进度，2019 年 5 月 22 日，控制中心云平台具备机房模块安装调试，开始进场安装。经过三个月紧张有序的安装、布线，2019 年 8 月 3 日，控制中心云平台送电成功，正式展开了云平台的调试工作。

作为国内第一个多线路、多业务的城轨云平台项目，没有成熟的经验可供参考，只有通过测试、研讨、论证摸索前行。经过招标阶段、设计联络阶段进一步细化方案，出现的许多技术细节都未得到充分验证。为了进一步验证城轨云安全可靠，满足云上业务资源需求以及兼容性要求等，经研究决定，呼和浩特市轨道交通公司于 2019 年 5 月至 8 月组织在呼和浩特市和林格尔县移动云计算中心搭建测试平台，根据项目实际配置，整体按照“硬件最小化，功能最大化”的思想，以呼和浩特云平台架构为基础，提取城轨云平台系统中的核心设备和典型设备作为最小系统，选取功能和接口全覆盖的最大子集作为首选模型，采用功能接口全部预留和增量式的整体架构，旨在按照项目实际需求做全面的测试，确保方案可行，功能、性能满足要求。

在和林测试平台完成全部测试工作的同时，主用中心云平台在控制中心完成自身部署，具备业务系统上云部署条件。业务系统上云部署期间，云平台配合业务系统开展各项测试工作，在前几轮测试的基础上，业务系统上云部署顺利开展，8月底完成1号线主要业务系统部署任务，云平台为业务系统提供了正常开展系统调试的条件。2019年10月底开始组织进行云平台单位工程预验收，11月23日，完成了云平台单位工程正式验收。

由于城市轨道交通云平台系统落地呼和浩特为全国首例，为保证整个建设期间设计及实施方案符合相关要求及规范，轨道交通公司自2019年2月至2019年12月多次组织召开专家评审会，邀请中国城市轨道交通协会、太原地铁、广州地铁、深圳地铁、济南地铁、青岛地铁、北京城建设计院、通号设计院、铁四院等各单位专家对设计方案、测试平台方案、实施方案等进行评审，会议上各单位专家提出了许多宝贵意见，同时也对项目研究的技术方案、项目进展情况、阶段性成果等给予了充分肯定。

9.4.2. 供货管理

云平台为ATS、ISCS、AFC、PIS等业务系统提供计算、存储、网络资源，是各业务系统进行调试的基础条件，所以其设备供货不仅要考虑自身安装、调试需求，还要满足各业务系统的需求。然而，设备供货受到合同签订、设计图纸、生产周期等因素影响，并且需要综合考虑运输时间、仓储条件、现场安装条件等。如何统筹协调、解决供需矛盾、满足项目需求，是设备供货管理的关键。

合理制定供货计划。第二次设计联络会期间，建设单位召集云平台集成商、供货商、安装单位、设计单位、监理单位、各相关业务系统共同商讨云平台供货需求，列出详细供货计划，经各方确认签字形成书面文件。供货计划中，应全面考虑甲供物资、甲控材料、线缆等。

严格落实供货计划。制定供货计划之后，严格按照计划督促集成商、供货商安排生产。首批设备生产完毕，监理立即组织出厂验收，按照合同要求严控设备质量，提出整改意见。为了确保生产进度满足计划，要求供货单位每周汇报生产进度，建设单位协调处理相关问题。提前落实仓储条件，督促现场设备机房移交进度，确保按计划具备安装条件。在设备供货管理中，必须做到实事求是。针对生产进度滞后、无法按期供货等问题，要商讨解决方案、提前应对处理，正面解决，如果拖延至计划节点时间才暴露问题，就会错失解决问题的时机。

适当调整供货计划。项目的执行是一个动态变化的过程，并非一成不变，即使制定了合理的计划，也难免在执行过程中做一些调整。由于控制中心云平台设备房供电、空调等条件制约，设备按期到货、安装后，仍无法上电调试。为解决此问题，对计划做出调整，将主用中心设备直接供应至和林云计算中心用于搭建测试平台，充分利用机房送电前的时间完成测试工作。在项目执行过程中，在满足最终目标和关键节点的基础上，应该根据项目实际情况动态调整计划。

9.4.3. 安装管理

云平台设备安装的主要范围在主用中心、灾备中心和站段。主用中心云平台承担了业务系统主要资源的提供，是正常运营模式下云平台的主要功能，其安装工作必须提前完成。灾备中心云平台主要实现部分业务系统的灾备功能，不影响综合联调、动调等工作，其安装工作可以放在最后，功能验收前完成即可。站段云平台与各业务系统的网络接口影响业务系统上云部署的功能实现，须尽早完成，确保各系统中心、站段联通。云平台设备安装须重点关注三部分内容，分别是：前置条件、安装进度和安装质量。

前置条件主要从设备、材料供货，机房环境等方面把控。设备、材料供货须严格按供货计划执行，确保计划节点；机房环境是云平台设备安装前重点把控的一个环节，须根据安装要求按时完成。地铁建设期机房环境普遍较差，而云平台基本都采用商用 IT 设备、非工业级产品，对安装环境要求较高，须按照数据中心机房标准进行建设。云平台做为各业务系统的基础，其安装工作须在业务系统调试前完成，而在这个阶段装修、通风、照明、正式电源等条件很难达到要求，所以机房环境是云平台设备安装过程中的一个重点问题，也是难点问题，需要尽早做出规划。本项目从以下三个方面进行把控：

第一，工作划分优先级。按照云平台主用中心、灾备中心、站段各项功能，从物理位置和设备类型上划分优先级，首先确保主用中心云平台的功能实现，这是整个云平台的核心；其次确保站段云平台网络设备功能及接口，这是云平台与业务系统、站段与中心联通的关键；最后确保站段与灾备中心的其他功能实现，完成云平台收尾工作。划分优先级、主次分明，按照重点依次抓，确保重要机房优先完成。

第二，重点机房提前抓。控制中心云平台机房是整个云平台的核心位置，无论交付时间还是机房环境都有严格的要求。云平台专业在机房设计阶段就参与方案的制定，建设单位组织云平台设计、监理、施工、厂家等技术人员，与机房建设相关设计、施工单位对接，特别是机房模块安装单位与机房建设单位的对接，从机房布局、空调设置、送风方式、顶面防水、地面保温、地板高度、净空高度、机柜排布、线缆布设、孔洞预留等全面沟通、确定方案，并在实施过程中严格监督，确保机房按需、按期、保质完成交付。

第三，见缝插针抢时间。由于控制中心土建、装修及机房配套设施整体安装工期紧，机房移交时间仍滞后于云平台设备到货时间，为了抢回工期，充分利用设备到货与机房移交的时间差，决定搭建测试平台进行各项安装、调试功能的测试验证，待正式环境具备后以最短的时间完成安装、调试工作。

在安装进度和质量的把控方面，严格按照计划进行，个别突破计划的节点，认真分析原因、积极探索解决方案，采取措施避免同类问题再次发生，并通过协调各方资源确保进度。在质量把控方面，充分利用监理单位、供货单位的力量实行项目内监督机制，通过监理旁站监督检查、供货单位安装督导，提前发现问题并责令整改，确保设备安装过程中设备防护到位、安装规范、接地良好，线缆敷设平整、绑扎规范、成端稳固、标识齐全，且整个过程与运营单位积极对接，及时发现不利于后期维护的问题并加以处理。

设备供货与安装阶段，制定科学的计划，合理安排工序、有效衔接，充分利用各方优势资源做好协调管理工作，为后续调试工作奠定基础，是确保工期、质量的重要手段。

9.4.4. 调试管理

一、控制中心云平台部署

控制中心云平台是云平台的核心部分，是业务系统上云部署的前置条件，所以控制中心云平台的调试是整体云平台调试的重点。

控制中心云平台部署调试的主要内容有：安全生产网部署调试、内部管理网部署调试、外部服务网部署调试、运维管理网调试以及机房动环系统调试。

城轨云平台搭建主要流程：

1. 按照优先安全生产网的原则进行搭建；
2. IT、数通现场人员分别对对应设备(服务器、交换机、防火墙)进行初始化配置；
3. 数通现场人员进行云平台管理网搭建；
4. IT 现场人员在云平台管理网络搭建完成后开始云平台软件（云管、虚拟化、桌面云）搭建；
5. 云平台搭建完成后，可通过云管理平台发放云资源；

城轨云平台部署及调试主要流程：

1. 确认云机房电源、空调运行正常；
2. 设备上电，数通设备配置调试完成；
3. IT 设备部署完成；
4. 双中心互联传输设备部署调试完成（含灾备中心调试内容）；
5. 输出设备调试报告；

业务系统虚机下发及上云测试流程：

1. 与各业务系统进行对接完成，确认需要资源；
2. 配合业务系统云上或云下测试完成；
3. 输出与各业务系统资源确认及测试完成记录

终端接入流程：

1. 物理链路打通：业务系统交换机通过各业务系统配线间云机柜内终端接入交换机实现终端接入物理链路打通；

2. 交换机、终端配置：配置好终端 IP 地址，在终端接入交换机上做好 VLAN 划分，在终端汇聚交换机上设置网关、配置终端访问网络路由指向；
3. 测试终端设备与云上、非云网络连通性；

非云接入流程：

1. 物理链路打通：业务系统交换机通过各业务系统配线间云机柜内 odf 配线架实现非云接入物理链路打通；
2. 交换机配置：和业务系统沟通后，确认交换机互联地址及业务系统所需访问网络路由指向；
3. 业务系统测试与所需访问网络连通性。

由于在测试平台已完成大部分测试工作，所以整个调试过程比较顺利，2019 年 8 月 3 日启动调试，8 月 19 日完成云平台自身部署，具备业务系统部署条件，各业务系统陆续开始部署。8 月底 1 号线 ATS 系统、ISCS 系统、集中告警系统、线网 PIS、ACS、公务电话基本完成部署，9 月初 AFC、MLC 基本完成部署。同时，已具备 2 号线 ATS、ISCS、集中告警系统的部署条件，提前为 2 号线业务系统提供基础，有效缩短 2 号线安装调试时间。

由于云平台属于成熟产品，且与业务系统进行过详细测试，所以控制中心云平台部署工作的关键在于前置条件的按时完成以及各业务系统需求的细化明确，如：机房建设、设备安装、线缆敷设、成端等必须满足调试条件的需求，否则会对进度和质量造成很大影响。业务系统资源配置、网络需求、安全策略需求等必须明确才能一气呵成完成部署工作。前置条件具备、资源需求明确后，云平台部署、配置相对比较容易且耗时较短。

二、站段云平台部署

站段云平台仅提供 ISCS、AFC、PIS 系统降级模式所需计算资源、存储资源，其部署、调试与控制中心云平台部署类似，相对更加简单。站段云平台调试工作中，与各业务系统的接口调试内容是重点，按照设计联络阶段确定的接口方案，将各业务系统与云平台网络打通，实现站段业务系统与中央级的联通，在中心业务系统资源发放完成后即实现业务系统的资源访问。此外，站段云平台调试需要施工单位及各业务接口单位积极配合，才可快速高效完成。

控制中心云平台、站段云平台部署完成，业务系统上云部署完成之后，如果业务系统自身调试完成，即可进行降级模式调试。降级模式调试主要由业务系统进行，云平台配合业务系统完成。

三、灾备中心云平台部署

灾备中心云平台部署、调试与控制中心安全生产网部署、调试内容类似，内容相对较少，主要包含安全生产网和运维管理网。完成部署后进行业务系统所需镜像制作，完成镜像制作即可根据业务系统调试情况开展灾备功能测试。

灾备中心部署调试的重点是主备中心网络联通，而后进行主备中心平台配置、业务发放、

业务部署、灾备功能测试，前置条件与控制中心类似。ATS 应用级灾备功能由信号系统进行测试，云平台配合提供条件，ISCS、AFC、PIS 等数据级灾备功能由云平台测试，业务系统验证功能。

四、业务系统上云部署

云平台自身部署完成后，协调云平台与各业务系统再次梳理确认系统资源提资情况，明确各业务系统网络互联情况，制定业务系统上云方案，组织开展业务系统上云部署工作。本阶段工作由业务系统牵头开展，云平台配合进行，需注意应安排各业务系统逐个与云平台对接，避免现场混乱，影响施工进度。在测试平台完成详细的业务系统上云部署测试后，现场部署相对比较容易，工作开展比较顺利，按照业务系统自身调试进度和现场情况陆续完成。业务系统部署上云后，业务接口需求导致云平台网络配置比较复杂，业务系统调试过程中遇到的网络问题排查比较困难，因此，必须协调好各业务系统和云平台配合好、共同开展部署及调试工作。

业务系统上云流程：

1. 业务系统提供提资需求表，云平台核对确认是否与设计一致；
2. 业务系统提供上云操作系统镜像，云平台根据镜像制作对应系统模板；
3. 根据业务系统提资表，云平台发放资源；
4. 业务系统登陆云资源确认，并开始进行业务系统部署。

五、资源分配

云平台向业务系统分配资源，是云平台功能实现的关键。在云平台部署完成，进行业务发放的过程中完成资源分配的操作，操作比较简单，关键在于资源分配的规划。本项目在用户需求书编制阶段就开始研究探讨资源的合理分配，基于目前主流业务系统的资源需求制定初版资源规划，经过多方论证、专项审查，优化资源配置。设计联络阶段，与各业务系统就资源配置进行详细的讨论，个别系统提出资源不足的问题，经过云测试平台的测试后，验证各业务系统资源基本满足使用需求。调试阶段按照规划很快完成资源分配，目前 1、2 号线各业务系统完成资源分配后，剩余资源较为充足，业务系统运行稳定。云平台具有易扩展、资源扩充较方便的特点，在运维过程中将持续对各系统资源使用率进行记录分析、合理调配。

六、功能测试

完成云平台部署调试以及业务系统部署之后，需进一步展开功能测试，主要包含云平台自身的功能测试和业务系统功能测试两部分。

云平台自身的功能测试是针对后期云平台运营维护进行的，主要包含：VDC 管理、配额管理、产品管理、VDC 自运维、云网络服务、弹性云服务器、镜像服务、云硬盘服务、系统资源监控、容量管理、租户资源监控、运维可视化、线下服务、纳管车站虚拟化、裸金属资源池管理、裸金属服务器使用、云硬盘高可用服务、云服务器容灾服务等。这部分功能在测试过程中，由运营单位、维保单位人员参与共同完成，在各项验收过程中也进行了详细测试，

发现的问题都进行整改复测，确保日后运维工作顺利开展。

业务系统功能测试项由业务系统主导进行，主要包含：资源确认、业务功能测试、接口功能测试、业务性能测试、稳定性测试、冗余功能测试、灾备功能测试等。这部分功能在各系统调试、综合联调、各系统验收过程中完成，云平台配合进行。过程中遇到云平台的问题由云平台进行整改，业务系统确认，最终实现功能。业务系统功能测试时需注意以下几点：

1. 云平台集成商收集各业务系统内部云上、云桌面、站段后备服务器、非云间的网络互访关系，根据各业务系统间互访需求，业务系统及云平台放通相应路由，并由业务系统进行验证；
2. 按照业务系统互访关系的复杂程度合理安排对接云平台顺序；
3. 根据规划，云平台和业务系统各自配置非云对接交换机互联 IP 并验证非云对接状态。

9.4.5. 验收管理

2019 年 9 月 27 日，呼和浩特市城市轨道交通云平台系统正式投入使用，具备承载 1 号线通 ISCS、AFC、PIS、CCTV、ACS、ATS、CAS、互联网售票、OA、车辆智能维护等多个业务系统能力，云平台运行良好，各业务系统使用正常。

2019 年 11 月 23 日，呼和浩特城市轨道交通云平台系统在呼和浩特建设工程质量监督站、呼和浩特市轨道交通公司、监理单位、设计单位以及相关参建单位的检查监督下一致验收，工程质量符合设计要求及相关验收规范。

由于呼和浩特城轨云平台是国内首个落地实施的城轨云项目，并没有完备的验收规范和相关标准指导项目验收，所以从项目执行过程中的现场检查、分部分项验收到最终的单位工程验收、项目验收，都要统筹做好规划，严格制定验收标准，确保项目的安全和质量。

呼和浩特城轨云平台规划为 1 个单位工程，划分主用中心云平台、灾备中心云平台、站段云平台三个分部工程，每个分部工程划分为管槽安装、线缆布放、设备安装、设备配线、电源与接地、软件安装、功能检验 7 个分项工程。在功能检验部分分别从安全生产网、内部管理网、外部服务网三个网域提供的功能和服务特点进行验收，确保云平台的基础性服务提供。单位工程验收的内容主要有以下几个方面：

1. 完成工程设计和合同约定的情况；
2. 工程技术档案和施工管理资料；
3. 工程所用钢管、桥架、光、电缆等材料和设备的进场试验报告；
4. 隐蔽工程验收记录、系统功能测试报告；
5. 主要分部（分项）工程质量验收情况；
6. 建设行政主管部门、质量监督机构或其他有关部门责令整改问题的执行情况；
7. 单位工程质量自评情况。

9.4.6. 企业管理

呼和浩特市轨道交通公司基于云平台建设的信息化一体化系统建设初期，要面对“云平台+大数据”贯穿建设全过程的领先要求，要面对轨道交通建设全过程 PPP 模式从管理界面、业务贯通和在云平台架构下部署及使用要求，高瞻远瞩地提出：在轨道交通中长期发展规划指导下统一规划、逐年滚动开展，数据集成、应用架构、基础设施和信息安全统一标准，对所有信息化项目统一规划投资，立项、设计、开发实施和项目管理统一管理和控制，采用集中式运维方式服务，充分共享基础设施资源，进行统一管理的“五统一”原则，即“统一领导、统一规划、统一技术标准、统一系统平台、统一组织实施”。

在此基础上，建立基于实现“资产管理统一、资产编码统一、信息平台统一”的企业管理服务一体化平台，从协同办公、人力资源管理、财务管理、合同管理、企业内部门户网站、资产管理 6 方面促进公司管理的信息化；建立支撑设备维修、客运组织、乘务、站务、票务管理、乘客服务等运营管理业务服务一体化平台，促运营服务信息化全面提升；建立包括数据标准、主数据管理系统、统一用户管理、企业服务总线的公共支撑服务一体化平台，除了实现跨平台的业务联动、数据交互，提升各个系统的协同处理效率外，可为后续企业信息化应用、大数据应用服务奠定基础。

呼和浩特市轨道交通公司的信息化系统一体化建设，充分考虑了呼市 PPP 模式下业务发展的要求，围绕“企业管理+运营管理”的核心建设思想，搭建信息化底层标准平台，相关子系统、子模块的考虑和设计，覆盖基本核心业务，以“最小投入、最优配置”为原则，从组织上打通了传统管理模式的壁垒，实现业务与技术管理的融合，促使各职能部门的管理职能由服务业务提升为引领业务发展，无意中显现出了“区块链”的特质：去中心化，任意节点之间的权利和义务都是均等的，每个人的工作行为从开始到归档都是公开的、被众人“监督的”；工作推进的点滴都被数据记录，相互协作更加主动，工作质量提高；可以降低维护成本，每一个节点在参与记录的同时也来验证其他节点记录结果的正确性，维护效率提高，成本降低。

9.4.7. 资源管理

呼和浩特城轨云基于“一云覆盖”的顶层设计理念，将物理分散的主用中心（位于控制中心）、灾备中心（位于三间房车辆段）、车站、车辆段/停车场等资源进行逻辑统一管理，利用软件定义的理念，将计算、网络、存储、安全等逻辑抽象为资源池，提供多站点的统一运维和运营管理能力。资源交付方式由传统硬件设备转变为更为细粒度的逻辑单元进行交付，从购买硬件、装机、上架等，转变为鼠标点击的“自助式交付”，分布式的技术手段配合全局管理，可实现按需分配、横向扩展、灵活变更、快速交付。

呼和浩特市轨道交通公司根据现有 1 号线运营生产经验，优化云平台现有资源，为云上业务系统新增需求提供计算、网络、存储资源等，实现业务系统快速部署，节省业务系统设备供货、安装、环境调试等硬件成本和时间成本。

一、呼和浩特-北京基于云平台的城市轨道交通支付“互联互通”

2020年6月5日，北京、呼和浩特两地实现轨道交通APP支付互联互通，为两地乘客提供了更便利和多元化的轨道交通互联网票务服务，提升了乘客选择的自由度。呼和浩特城轨云平台快速响应AFC系统资源需求，为京蒙两地实现APP支付互联互通提供基础环境，实现“让数据多跑腿”，深化“京蒙合作”、积极融入“京津冀一体化”发展作出了智慧探索。

二、基于云平台的呼市城市轨道交通1、2号线信号系统“互联互通”交叉测试平台

2020年8月5日，基于云平台的呼和浩特市城市轨道交通1、2号线信号系统“互联互通”交叉测试平台在三间房车辆段培训楼搭建完成，投入测试使用。该平台利用云平台灾备中心资源，遵循既有ATS系统设计原则，云平台厂家利用一周时间完成搭建，满足信号系统互联互通设计需求，同时为信号系统厂家有效降低硬件成本、节省部署时间。

9.5. 未来方向

呼和浩特城轨云平台系统作为国内首个“多线路、多业务”城轨云，在多方共同努力下顺利建成落地，践行了“云计算+城轨”的发展理念，用云计算、大数据技术为城市轨道交通提供地铁运营生产、企业管理、建设管理、运营管理以及资源管理等服务。

基于目前以IaaS层服务为主的“呼和浩特城轨云1.0”向城轨云2.0方向的发展演进可分成2个层面：

第一个层面是对既有平台的优化，包括1、完善既有平台架构，提高资源使用率，扩展企业信息化应用领域。2、体系化云平台管理框架，针对城轨云运维，提出更合理的管理和办法（如架构、职责、人员等）。

第二个层面是面向未来的智能/智慧应用的。城轨云2.0要在共享基础设施资源的基础上，构建共通标准、共享数据、共享服务，适应业务的快速变化以及新接入模式/新商业模式的应用体系，实现技术、业务、商业模式的综合创新。重点建设PaaS平台，引入数据中台、算法中台，按照统一的数据标准与服务标准，实现对各子系统数据进行采集与汇入。通过对数据进行规范治理、建模、存储，最终对外以公共接口的方式提供数据服务。数据中台将各业务系统的算法抽象并封装，这些算法不仅包含传统的统计算法，还包含基于大量数据的深度学习算法。“呼和浩特城轨云2.0”不仅是对平台的升级，更是向智慧城轨的迈进，计划引入新的智能应用，建设智慧撑城轨，智能应用包括：

一、智能调度

综合智能调度(面向立体信息和自主决策的全自动综合调度系统)是指通过将不同调度角色联动功能自动化、调度界面整合化等手段实现调度员角色的整合，通过对多专业多维度立体信息的分析，实现自主决策的全自动综合调度系统。

基于“呼和浩特城轨云2.0”中数据平台的多源信息融合与处理，结合算法中台实现智能认知与诊断，达到多目标快速优化决策、人机界面友好交互的目标，最终实现建设以指挥行

车为核心的全自动智能调度系统，并促进调度岗位职能的进一步融合。全自动智能调度系统将能够在故障及应急条件下，辅助综合调度员完成故障诊断、辅助决策、信息自动报送发布与统计等工作，大幅提升城轨调度指挥的自动化、智能化水平，在保障安全的前提下，降低运营维护成本，全面提升系统运输效率和应急处置能力，并为乘客提供高效便捷的服务。

二、智能运维

智能运维是结合轨道运营系统、可操控管理平台实现对轨道运营系统信息进行处理、诊断及故障解决的过程，其主要服务于城市轨道交通日常运营与维护。

通过“呼和浩特城轨云 2.0”中数据中台实现对运营数据的汇总与处理、设备状态数据的采集及检测，引入算法中台的相关算法模型，实现对列车运行过程中故障的智能诊断、对设备健康状态评估、对设备全寿命周期管理等功能。

三、智慧车站

智慧车站是在“呼和浩特城轨云 2.0”基础上，集车辆、信号、供电、通信、综合监控、云平台及 AFC 等多个专业的综合性应用，实现车站设施设备状态监控（包括远程功能），帮助工作人员及时、准确把控设备运行状态、故障趋势、维修计划，实现“一键开闭站”；其次，通过将行调、电调、环调所需信息进行汇总，形成应对场景的操作列表，降低操作复杂度，提高应急场景处理的准确度。

10. 附录

10.1. 测试结果

10.1.1. 云平台自测试结果

云平台自测试，主要包含运营管理、云服务、运维管理、云桌面四个方面进行，测试用例 100%测试通过，具备业务系统上云部署测试的条件。

10.1.2. 业务系统功能及兼容性测试结果

针对 ATS、ISCS、PIS、AFC、ACS、CAS 等业务系统功能及兼容性测试，测试结果表明各业务系统功能正常，无软件无法运行、异常崩溃等兼容性问题，业务系统与平台兼容性满足要求。

10.1.3. 系统性能测试结果

10.1.3.1. 云平台虚拟机性能

1. 对云上虚拟机进行 IO 读写测试
2. 通过 iperf 的软件，持续运行 180s 测试网络带宽
3. 通过两个虚拟机间传输大块数据测试虚拟机间传输速度
4. Windows 系统启动 mtr 丢包测试工具，持续 180s 向服务器发送数据包测试丢包率

云平台虚拟机性能测试结果

测试项	测试结果	备注
IO 吞吐量	1465.17MB/S	
网络 IO	949Mbps	
传输速率（云上虚机间）	536M/S	
传输速率（云上桌面间）	647M/S	
丢包率	0	

测试结果显示云平台提供的单虚拟机性能优良。

10.1.3.2. 云平台 ATS 性能测试

1. 测试环境：

- 1) 搭建 1 号线全线设备从三间房车辆段至坝堰村停车场包含正线 7 个集中区至共 19 个车站（实际项目车站采用物理机部署，实验室采用 19 个站段云方式进行部署）
- 2) 放置全线 24 列车，按大交路计划运行图运行（西二环路至坝堰村）
- 3) 连续运行时间超过 10 小时

2. 测试结果：

- 1) 无列车降级、通信中断等异常情况，云平台资源使用稳定，具备主用中心上线条件

1 号线 ATS 各服务器性能测试条件下资源使用情况

业务系统	设备名称	配置		CPU 使用率 (%)			内存使用率 (%)			网络流入速率 (KB/s)			网络流出速率 (KB/s)		
		VCPU	内存	最大值	最小值	平均值	最大值	最小值	平均值	最大值	最小值	平均值	最大值	最小值	平均值
ATS 一号线	应用服务器 1	4	8	8.40%	2.37%	6.00%	45.46%	5.75%	22.00%	145.51	39.84	68	211.52	121.58	161
	应用服务器 2	4	8	6.21%	4.53%	5.00%	19.00%	17.11%	18.00%	74.57	34.35	56	64.5	11.7	21
	通信前置机 1	4	8	1.69%	1.16%	1.50%	36.40%	26.76%	27.00%	31.81	10.59	22	15.78	1.77	5
	通信前置机 2	4	8	1.60%	1.21%	1.50%	29.01%	28.02%	28.00%	31.99	9.04	24	3.38	1.86	2
	调度工作站 1	4	8	13.11%	3.10%	10.00%	29.75%	24.08%	27.00%	28.83	14.29	20	28.95	11.32	20
	调度工作站 2	4	8	13.49%	2.89%	10.00%	26.32%	24.58%	25.00%	26.94	2.48	20	28.47	3.98	10
	调度长工作站	4	8	11.98%	2.61%	11.00%	38.60%	22.03%	25.00%	26.59	1.2	24	7.48	0.81	7
	计划工作站	4	8	3.88%	0.75%	3.50%	28.19%	26.02%	27.00%	2.38	1.4	1.8	2.3	0.8	1.5
	灾备-应用服务器 1	4	8	5.62%	0.72%	5.00%	50.18%	11.48%	15.00%	29.66	8.58	20	8.97	2.11	8.8
	灾备-应用服务器 2	4	8	5.96%	0.61%	5.00%	51.60%	11.63%	45.00%	29.65	5.08	20	9.12	2.99	9
	灾备-通信前置机 1	4	8	0.45%	0.11%	0.40%	8.40%	7.43%	8.00%	10.8	0.1	10	13.37	0.1	13
	灾备-通信前置机 2	4	8	0.40%	0.10%	0.40%	8.28%	7.51%	8.00%	9.26	0.1	9	13.38	0.1	13

10.1.3.3. 云平台 ISCS 性能测试

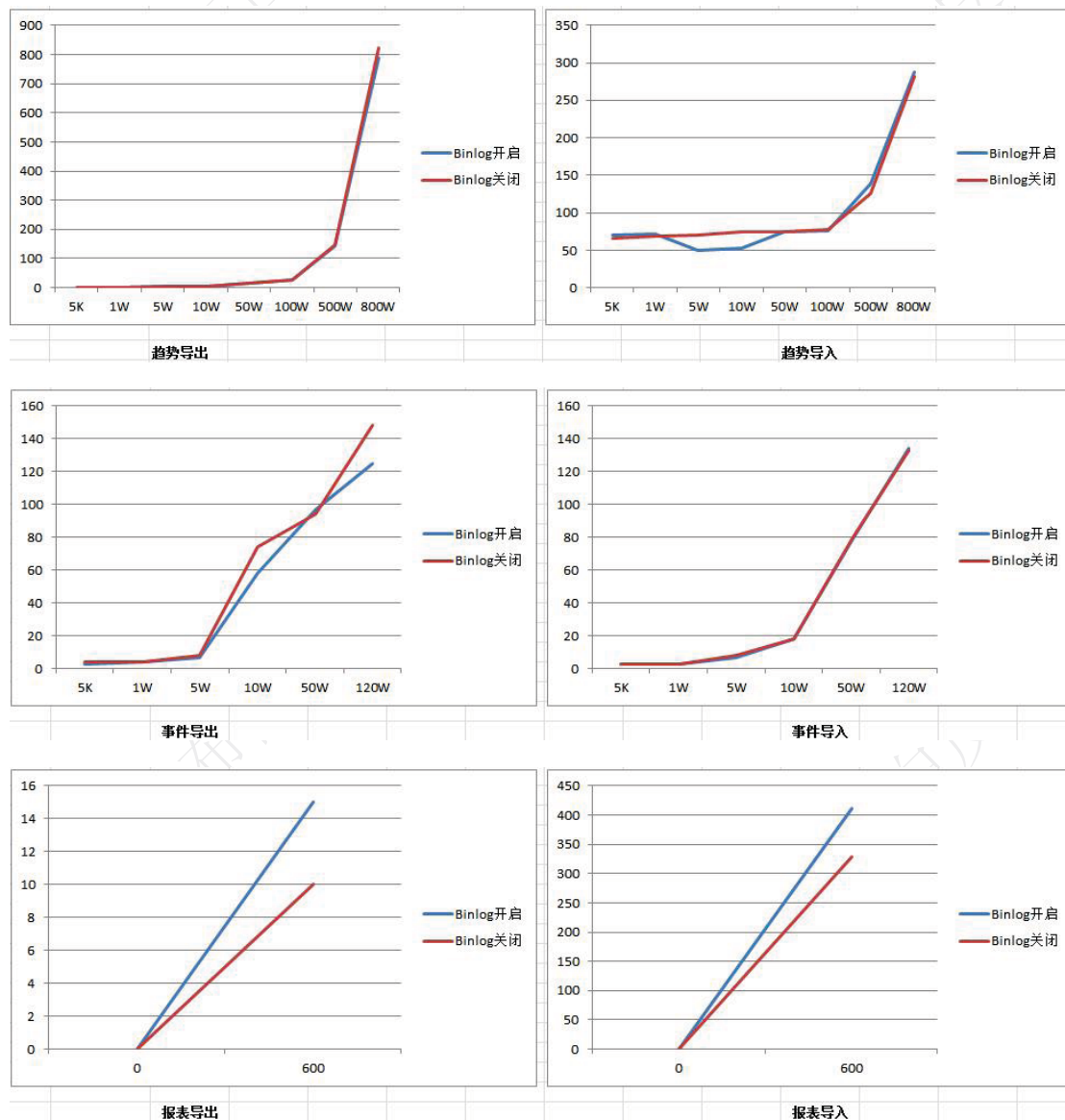
1. 云平台 ISCS 历史数据管理性能测试

1) 测试环境

针对历史服务器中存储的综合监控数据，包括历史事件、趋势、报表，导入导出不同规模大小的数据量，记录和分析耗时性能。

2) 测试结果

CPU 核心数和内存容量大小可承载该数据量压力，实时性指标符合业务规格要求。



2. 云平台 ISCS 实时性性能测试

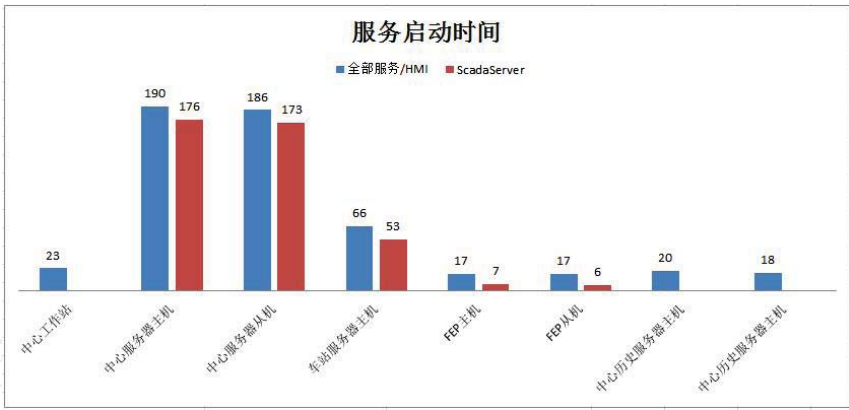
1) 测试环境

工程数据组态 50 万 I/O 点，且中心服务器部署 20 万点、车站服务器部署 10 万点，FEP

部署 1 万点，对 HMI 和实时服务启动时间、切图时间、HMI 读写数据时间等性能进行测试。

2) 测试结果

实时服务器和 FEP 在线服务、工作站 HMI 的启动时间统计数据如下，实时性指标符合业务规格要求。



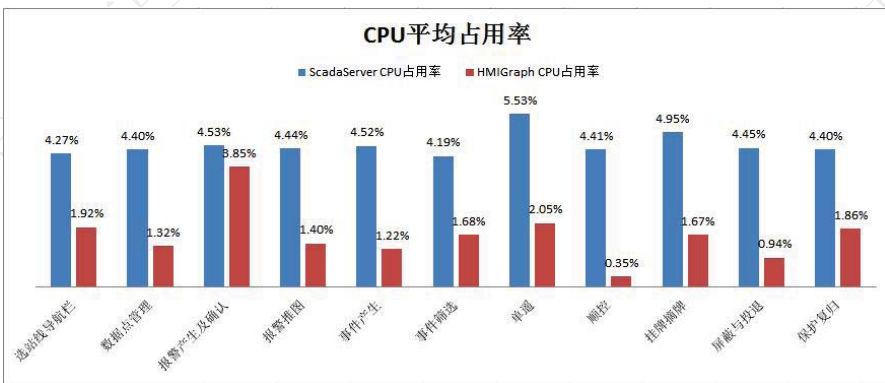
3. 云平台 ISCS 服务性能指标拷机测试

1) 测试环境

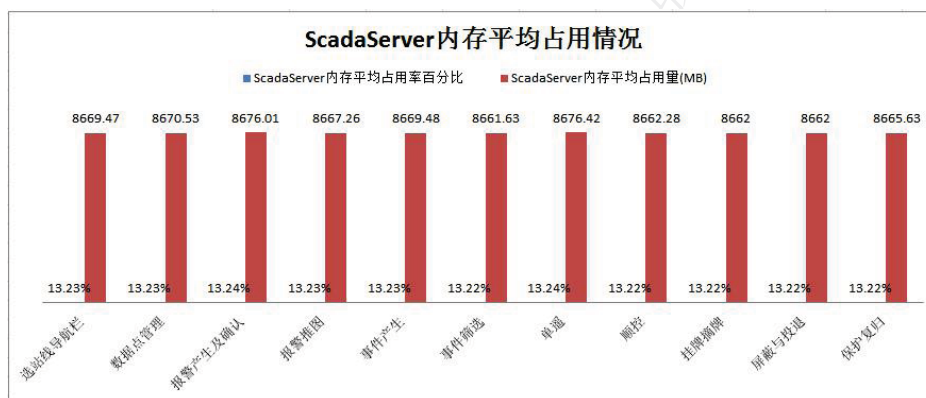
服务器硬件配置，对综合监控常用的业务场景进行长时间拷机压力测试，以及对服务器部署数据点总数的 20%、40%和 80%的点进行随机模拟，记录工作站、FEP、实时服务器的整机内存使用率、CPU 占用率和带宽、业务进程 ScadaServer 的内存使用和泄露、占用率等，并分析指标趋势。

2) 测试结果

服务器对于业务数据处理能力在长时间不间断拷机下无大量堆积，各业务的资源指标和实时性指标符合业务规格要求。



ScadaServer 进程 CPU 平均使用率为 5%左右 HMI Graph 进程 CPU 平均使用率为 2%左右



ScadaServer 进程内存平均使用率为 8670M，内存平均占用率 13%左右

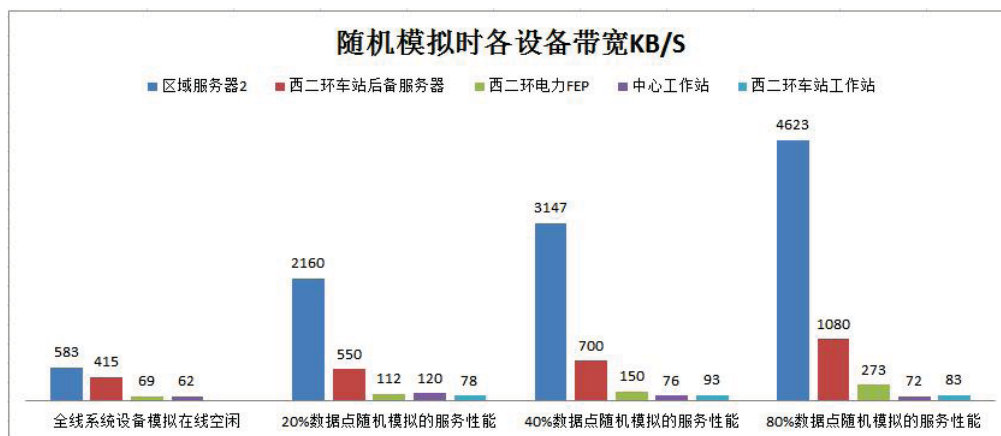
4. 云平台维度 ISCS 整机性能指标统计

1) 测试环境

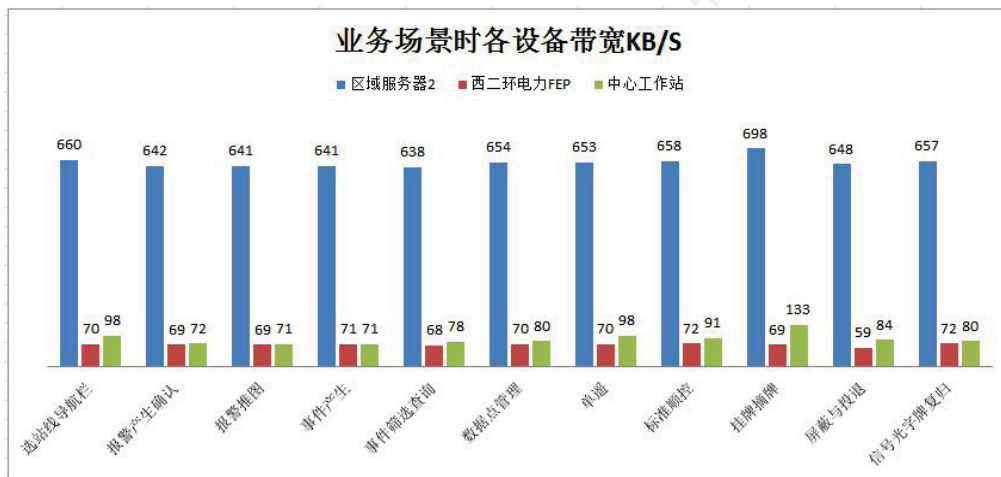
云平台维度（含操作系统进程）性能指标监控统计，使用云平台系统工具统计测试过程中各场景的整机平均 CPU、内存占用率以及带宽。

2) 测试结果

服务器对于业务数据处理能力在长时间不间断拷机下无大量堆积，各业务的资源指标和实时性指标符合业务规格要求。



不同数据量设备带宽使用情况



上图 不同业务场景设备带宽使用情况

下表 ISCS 各服务器性能测试资源使用情况

测试场景	测试时间	拷机设备	机器配置		CPU(平均值)%	内存（平均值）GB	
			CPU	内存	整机	整机	内存占百分比
测试场景	120 分钟	区域服务器 2	16	64	3.37	7.87	12.30
		西二环车站后备服务器	8	16	3.535	4.06	25.37
		西二环电力 FEP	4	4	2.98	1.02	25.62
		中心电调	8	16	8.87	0.58	3.64
	60 分钟	区域服务器 2	16	64	19.14	11.28	17.62
		西二环车站后备服务器	8	16	23.98	4.55	28.46
		西二环电力 FEP	4	4	3.96	1.07	26.85
		中心电调	8	16	2.815	0.36	2.25
		西二环车站工作站	8	16	1.725	0.32	1.97
	60 分钟	区域服务器 2	16	64	23.3	16.14	25.22
		西二环车站后备服务器	8	16	29.67	5.87	36.67
		西二环电力 FEP	4	4	4.48	1.08	26.88
		中心行调	8	16	5.69	0.67	4.19
		西二环车站工作站	8	16	1.84	0.32	2.01

80%数据点随机模拟的服务性能	60 分钟	区域服务器 2	16	64	29.2	33.75	52.74
		西二环车站后备服务器	8	16	36.48	9.96	62.26
		西二环电力 FEP	4	4	7.72	1.31	32.73
		中心行调	8	16	6.3	0.67	4.22
		西二环车站工作站	8	16	1.78	0.32	2.01

5. 云平台 ISCS 信息安全测试

1) 测试环境

- a. 部署安全管理平台、工控安全监测审计系统、终端管理软件
- b. 模拟 1、2 号线单驱动器日志数据进行发送

2) 测试结果

综合监控信息安全业务测试验证功能点具备，安全管理平台和工控安全监测审计系统内存使用率较高，业务系统建议将内存由 32G 调整为 64G，目前主用中心内存富余，可按业务系统建议调整内存。

ISCS 信息安全性能测试资源使用情况

业务系统	设备名称	机器配置		CPU 使用率 (%)			内存使用率 (%)		
		CPU	内存	最大值	最小值	平均值	最大值	最小值	平均值
信息安全	安全管理平台	16	32	0.16%	0.13%	0.15%	67.61%	67.01%	67.30%
	工控安全监测审计系统	16	32	7.50%	1.01%	1.05%	79.28%	72.45%	77.00%
	终端管理软件	4	8	5.58%	4.98%	5.00%	36.33%	23.38%	13.00%

10.1.3.4. 云平台 ACS 性能测试

1. 测试环境

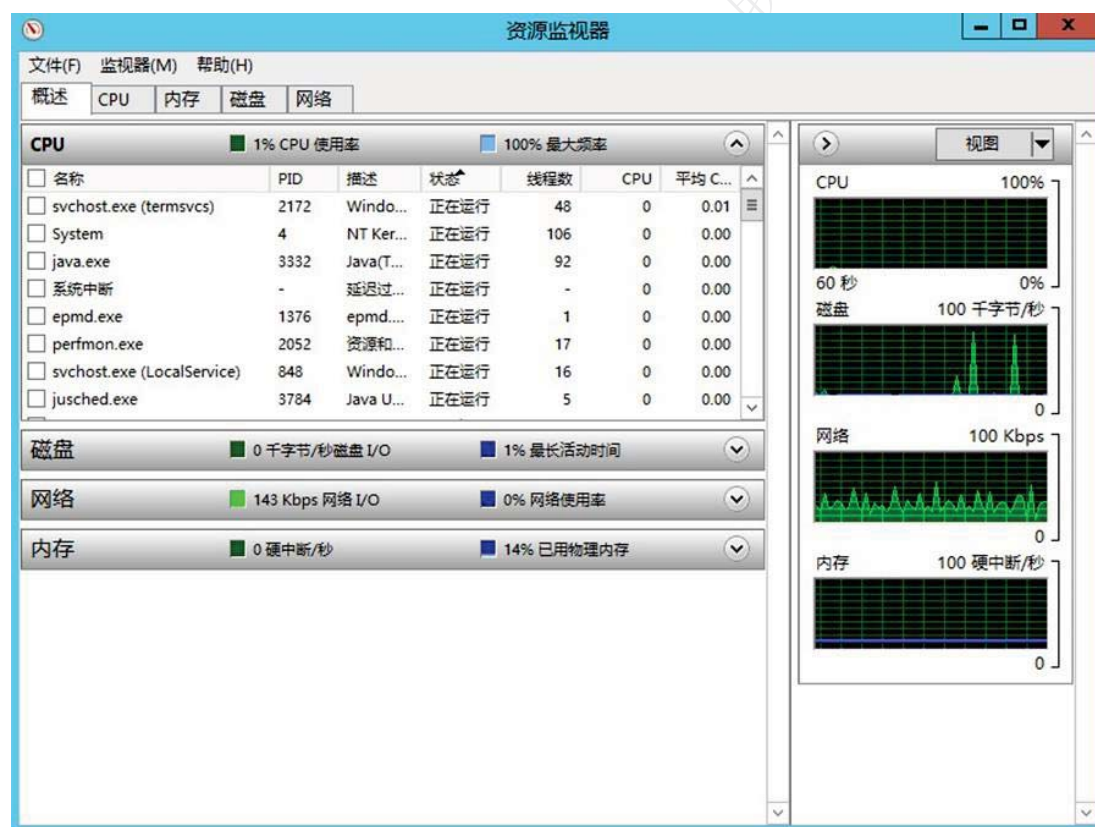
平台下发 1 万个持卡人到线路服务器，查看每台服务器的运行情况。

2. 测试结果

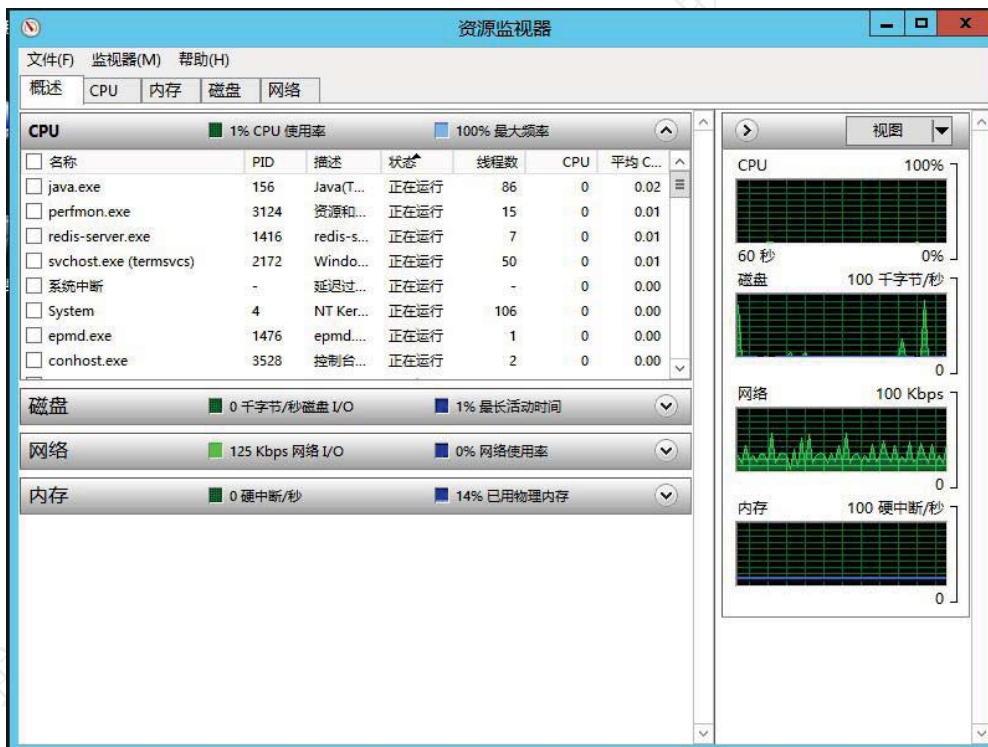
压力测试各服务器运行正常。

ACS 各服务器性能测试资源使用情况

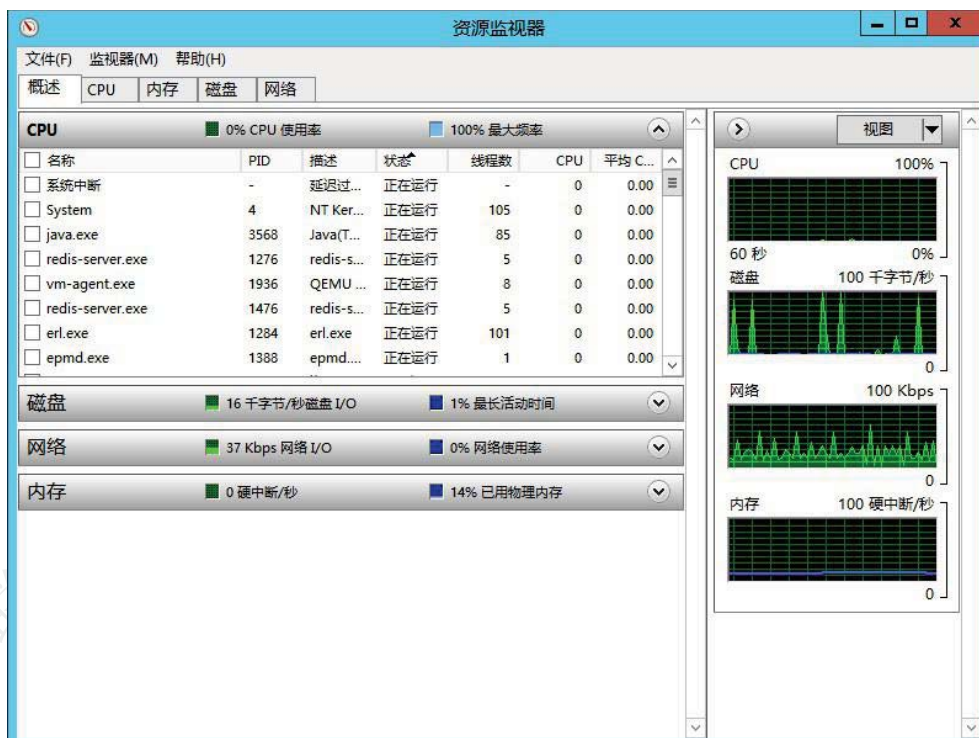
设备	CPU	内存	网络	内存使用率	CPU 使用率
应用服务器 A	8	16G	143kbps	14%	1%
应用服务器 B	8	16G	125kbps	14%	1%
应用服务器 C	8	16G	37kbps	14%	1%
负载均衡服务器 A	4	8G	10kbps	12%	1%
负载均衡服务器 B	4	8G	2kbps	14%	1%
数据库服务器 A	4	8G	69kbps	27%	2%
数据库服务器 B	4	8G	269kbps	26%	2%



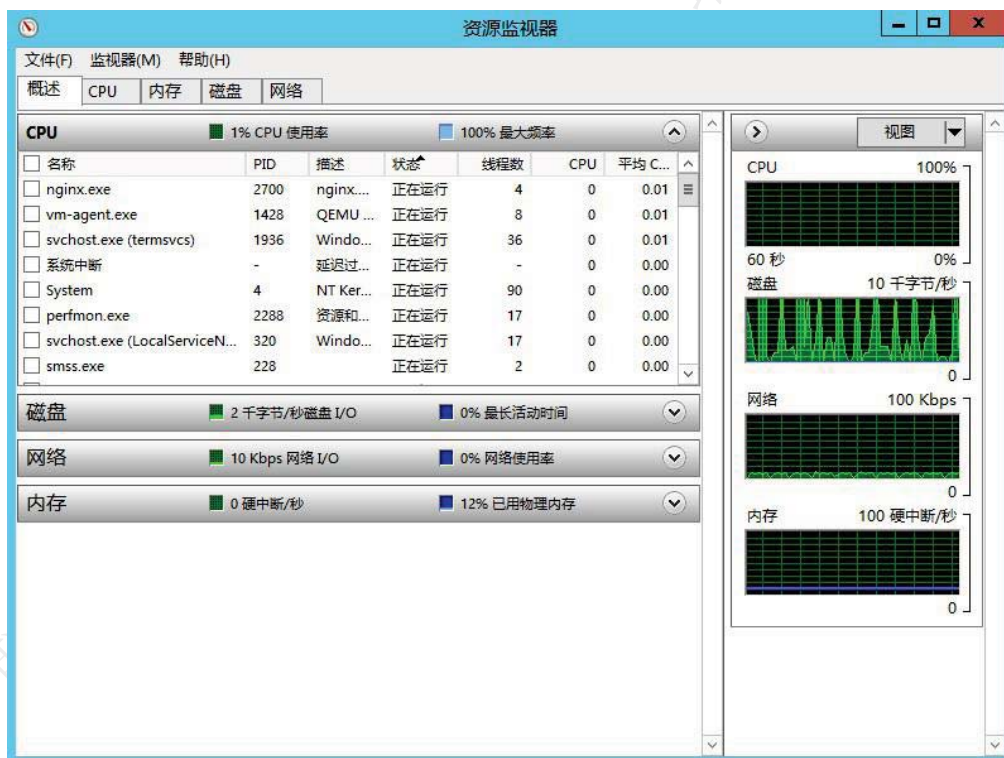
应用服务器 A 资源使用情况



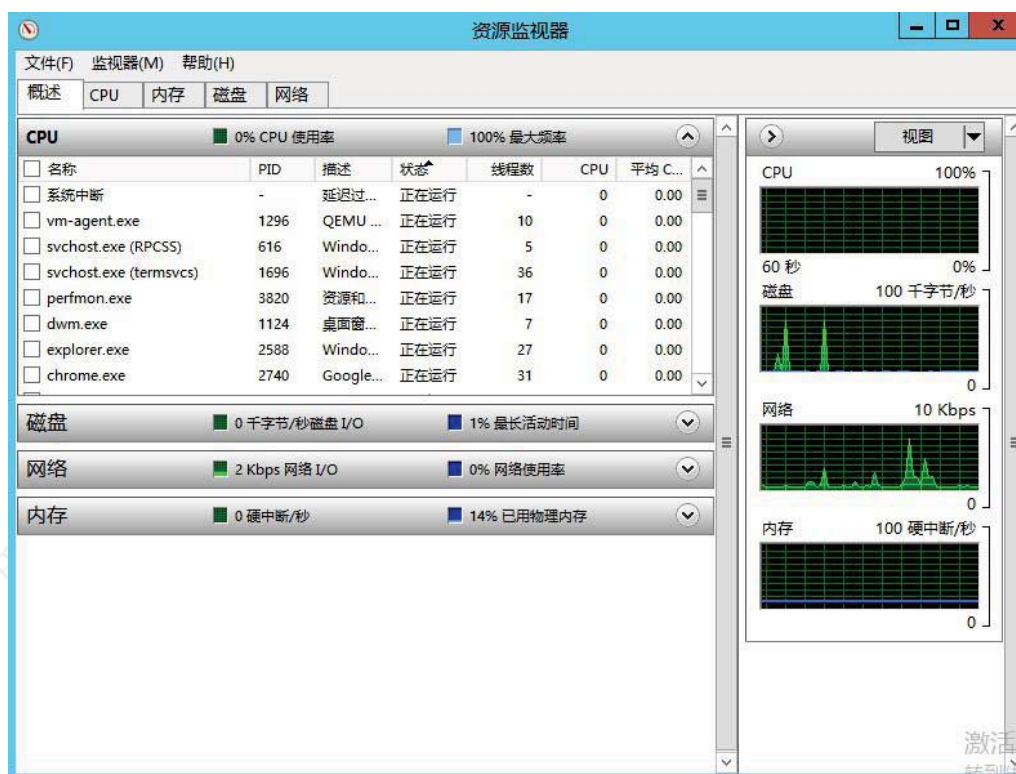
应用服务器 B 资源使用情况



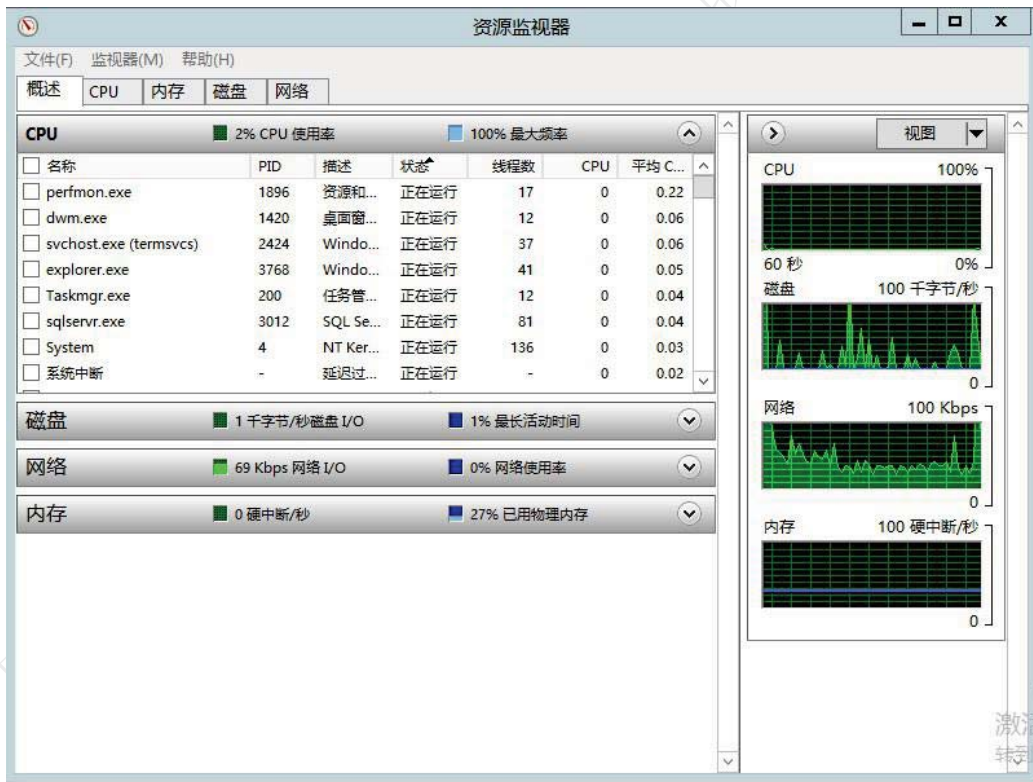
应用服务器 C 资源使用情况



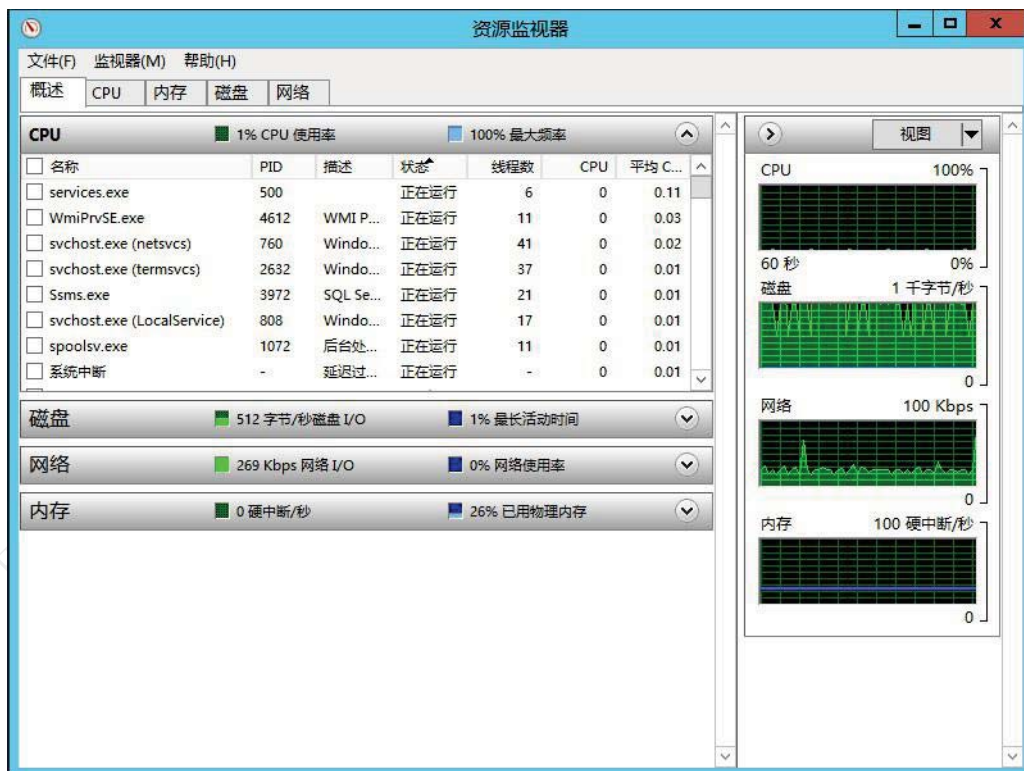
负载均衡 A 资源使用情况



负载均衡 B 资源使用情况



数据服务器 A 资源使用情况



数据服务器 B 资源使用情况

10.1.3.5. 云平台 PIS 性能测试

1. 测试环境

ISCS、ATS 进行性能测试时，将数据同步接入 PIS，测试编播中心、线网中心、车站、车载各功能正常运行，统计各设备资源利用情况。

2. 测试结果

压力测试各服务器运行正常，各服务器 CPU 及内存资源使用率基本在 15%以内，分配资源满足业务系统需求。

PIS 各服务器性能测试资源使用情况

业务系统	设备名称	虚拟机 CPU/ 内存规格	CPU 使用率 (%)			内存使用率 (%)			网络流入速率 (KB/s)			网络流出速率 (KB/s)		
			最大值	最小值	平均值	最大值	最小值	平均值	最大值	最小值	平均值	最大值	最小值	平均值
PIS	应用服务器	64CPU128G	0.65%	0.60%	0.62%	7.10%	7.00%	7.00%	50	49	50	0.01	0.01	0.01
	编播工作站	32CPU32G	11.41%	7.98%	10.00%	12.14%	10.03%	10.50%	400	400	400	52	52	52
	数据库服务器	64CPU128G	6.21%	2.57%	4.57%	16.21%	10.39%	15.50%	264	50	260	1189	0.01	1000
	接口服务器	32CPU32G	14.47%	0.87%	14.00%	7.10%	5.66%	7.00%	50	49	50	0.34	0.01	0.1
	车站服务器	32CPU32G	13.17%	12.13%	13.00%	11.42%	11.14%	11.20%	54	50	51	399	380	390
	灾备-数据库服务器	64CPU128G	4.1%	2.57%	3.57%	12.61%	9.87%	11.00%	220	50	210	550	150	500

10.1.3.6. 云平台 AFC 性能测试

1. 云平台 AFC 文件传输压力测试 (8CPU16G 内存)

1) 测试环境

根据业务需求，模拟 SLE 终端设备(AGM、TVM、BOM)从 MLC 接入服务器上传交易、业务、事件、审计文件，本次测试机器四台，每台模拟 60 个 SLE 终端设备，共 240 个设备。

在 SLE 终端设备分别模拟 AGM 、 TVM、 BOM 分别向 MLC 接入服务器上传交易、业务、事件、审计文件，本次测试机器四台，单台机器在十分钟内向 MLC 接入服务器上传 10 万交易文件，采集测试结果数据。

2) 测试结果

单个接入点 240 个线程 20 分钟上传 28.8 万交易数据,上传成功率 99.46%。

模拟 AG,BOM,TVM 共 240 个线程循环下载全量参数和程序文件 20 分钟,成功率 100%。

socket 长连接 240 个线程,每秒 240 个状态数据循环上传 20 分钟,所有上传均收到反馈,无堵塞情况。

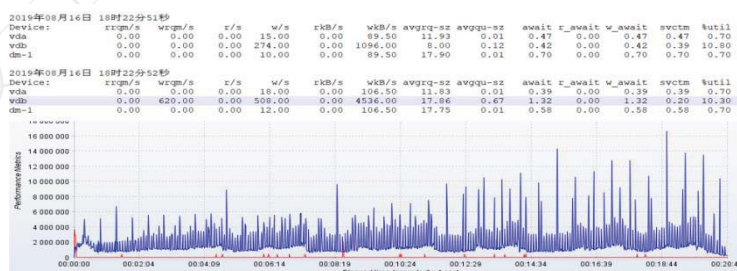
CPU 在高峰冲击下达 40%, 内存利用率达 15%, 在瞬间部分事物的响应时间高达 60s, 8VCpu 和 16G 内存可以满足系统基本要求。



CPU 使用情况



内存使用情况



内存使用情况

2. 云平台 AFC 消息传输压力测试(32CPU64G 内存)

1) 测试环境

根据业务需求，模拟生产者发布消息的 14 种情况，涉及全部业务，运行时长：3 小时，总消息量：9054K，并发数：1500 个/s（2 条线）。

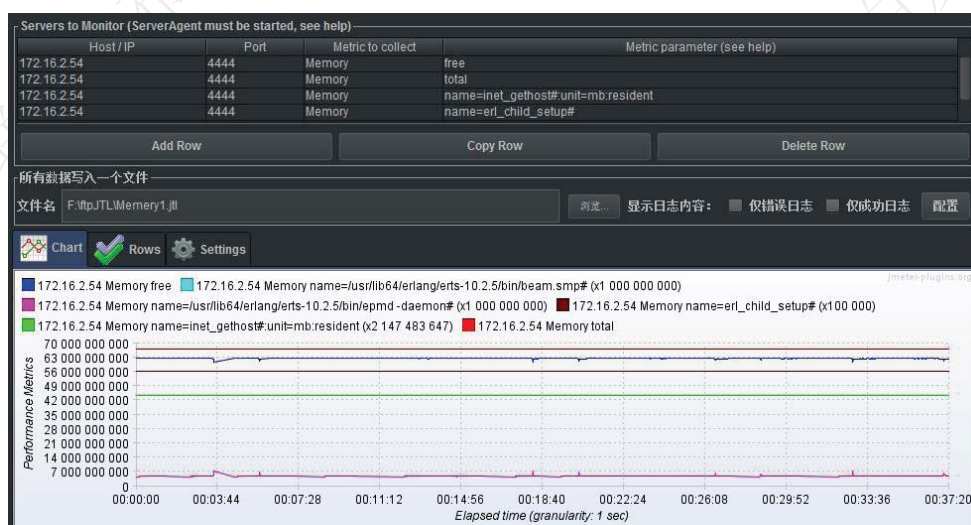
根据实际业务需求，模拟业务场景，进行业务逻辑控制，执行测试，让系统持续运行 3 小时，监听、记录和检查测试结果数据；在测试过程中，采集 MLC/ACC MQ 系统及其云平台服务器的测试结果数据和 web 管理工具监控数据，并保存相关测试结果数据，为性能调优提供系统真实运行数据。

2) 测试结果

吞吐量为 5619 个/S，单个消息成功发布消费的平均响应时间 1.71ms，消息成功发布消费的正确率 99.97%，均已达到预期业务性能指标，内存利用率 6.81%，CPU 利用率在瞬间压力情况下，会达到 70%、稳态为 45%，满足服务 MLC/ACC MQ 系统。



压力测试 CPU 使用情况



压力测试内存使用情况

AFC 各服务器性能测试资源使用情况

设备名称	实验室配置		CPU 使用率 (%)			内存使用率 (%)		
	VCPU	内存	最大值	最小值	平均值	最大值	最小值	平均值
ACC_TAC	8	8	2.27%	0.65%	0.80%	50.77%	36.11%	48.00%
ACC_LINE2_生产网 1	8	16	0.04%	0.03%	0.04%	6.43%	5.25%	6.00%
ACC_LINE2_生产网 2	8	16	0.04%	0.03%	0.03%	6.18%	5.65%	6.00%
ACC_LINE2_生产网 3	8	16	0.03%	0.03%	0.03%	6.35%	5.74%	6.00%
ACC_LINE2_生产网 4	8	16	0.03%	0.03%	0.03%	6.33%	5.86%	6.00%
ACC_LINE2_票务 1	8	16	0.06%	0.05%	0.05%	8.91%	15.79%	13.00%
ACC_LINE2_票务 2	8	16	0.04%	0.04%	0.04%	9.91%	6.84%	8.00%
ACC_LINE2_MLC_接入_01	16	32	40.11%	0.27%	30.00%	5.87%	4.28%	5.00%
ACC_LINE2_MLC_接入_02	16	32	100.00%	0.11%	65.00%	5.91%	4.08%	5.00%
ACC_LINE2_MLC_接入_03	16	32	0.03%	0.03%	0.03%	6.09%	3.45%	5.00%
ACC_LINE2_MLC_接入_04	16	32	100.00%	0.03%	90.00%	5.40%	3.54%	5.00%
ACC_LINE2_MLC_接入负载均衡 1	16	32	0.27%	0.10%	0.15%	5.88%	3.43%	5.00%
ACC_LINE2_MLC_接入负载均衡 2	16	32	0.03%	0.03%	0.03%	6.32%	3.84%	5.00%
ACC_LINE2_MLC_传输管理系统	32	64	35.98%	0.07%	20.00%	23.69%	2.51%	4.00%
ACC_LINE2_MLC_外部接入系统	8	16	0.75%	0.11%	0.30%	12.46%	9.05%	5.00%
ACC_LINE2_MLC_运营管理子系统	8	16	2.39%	0.05%	1.00%	10.13%	5.29%	7.00%
ACC_LINE2_MLC_设备管理子系统	8	16	0.99%	0.04%	0.50%	10.81%	5.96%	8.00%
ACC_LINE2_MLC_数据处理子系统	8	16	0.60%	0.04%	0.50%	13.34%	8.97%	12.00%
ACC_LINE2_ACC_ISAM	8	8	3.08%	0.63%	1.00%	61.25%	39.49%	50.00%
ACC_LINE2_ACC_传输管理	8	32	9.77%	0.07%	7.00%	35.19%	2.67%	5.00%
ACC_LINE2_ACC_接入	8	32	0.25%	0.04%	0.05%	11.94%	8.33%	10.00%
ACC_LINE2_ACC_清分管理子系统	8	16	2.55%	2.28%	2.40%	5.81%	5.61%	5.70%
ACC_LINE2_ACC_数据管理子系统	8	16	0.23%	0.04%	0.04%	12.11%	6.84%	10.00%

ACC_LINE2_ACC_数据处理子系统	8	16	0.23%	0.04%	0.04%	12.37%	8.59%	11.00%
-----------------------	---	----	-------	-------	-------	--------	-------	--------

城轨云平台及云平台承载的业务系统性能测试结果表明，城轨云平台架构设计满足城市轨道交通需求，为业务系统分配的计算、网络、存储资源满足业务系统需求，部分业务系统如 AFC 部分服务器在极限压力下资源使用率较高，后续根据现场情况进行动态调整，大部分业务系统分配的资源仍存在较大压缩空间，随着城轨云平台的建设及普及，可极大地提升资源利用率。

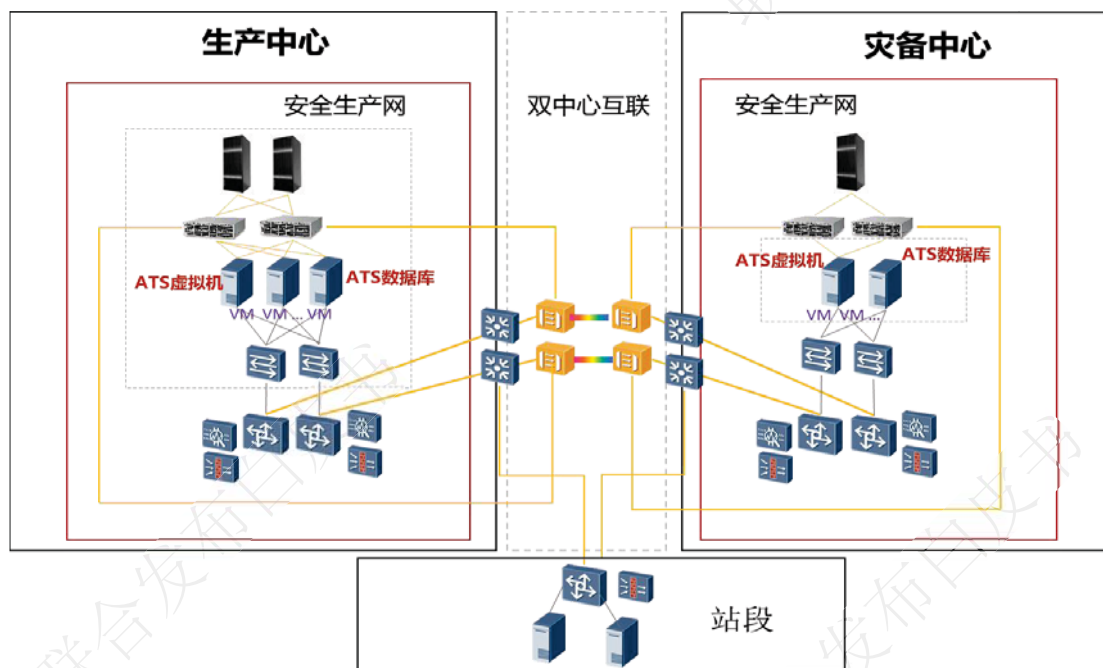
10.1.4. 灾备测试结果

针对灾备测试，根据业务系统不同分别进行应用级灾备测试和数据级灾备测试，ATS 进行应用级灾备测试，ISCS、AFC、PIS 和 ACS 进行数据级灾备。

10.1.4.1. 应用级灾备测试

应用级灾备主要验证 ATS（1、2 号线）的应用级灾备测试，须验证在主用中心不可用的情况下，灾备中心可接管 ATS 业务，测试步骤如下：

1. 主用中心 ATS 部署调度工作站、计划工作站、应用服务器、裸金属数据库服务器、通信前置机
2. 灾备中心部署备控应用服务器、备控裸金属数据库服务器、调度工作站（物理 PC）
3. 根据 ATS 业务系统网络架构，主用中心和灾备中心分别为固定 IP，站段 ATS 车站分机同步将车站数据发送主备控制中心应用服务器，双中心应用服务器为主备关系
4. 模拟主用中心不可用场景（关主用中心设备）
5. 备控中心应用服务器由备用状态切换为主用状态，系统正常切换至备控中心，通过车站分机与备控中心应用服务器、调度工作站数据通道实现备中心 ATS 相关调度操作。



ATS 应用级灾备网络架构

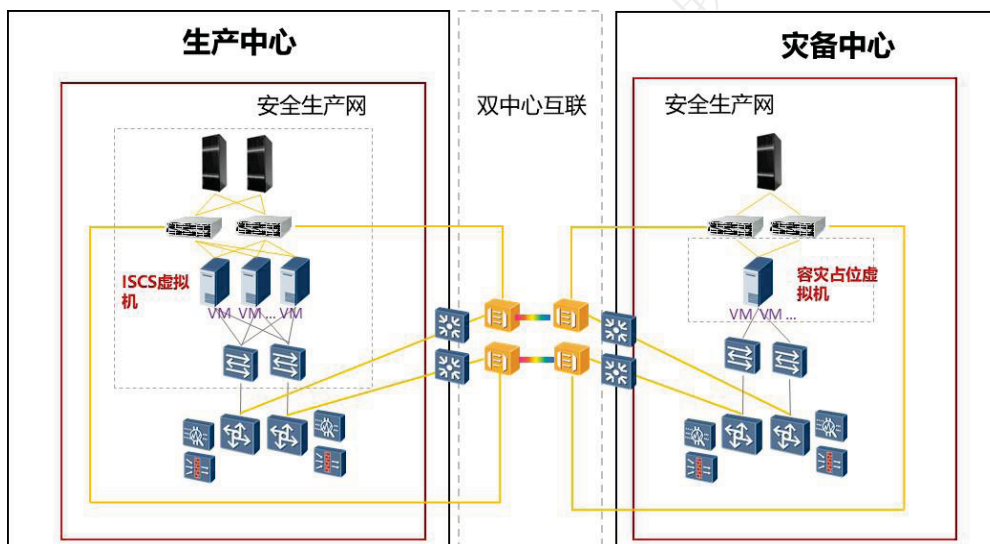
测试结果显示主用中心 ATS 设备故障情况下，ATS 可秒级切换至灾备中心应用服务器及调度工作站，ATS 车站设备应用无感知不影响正常控车运行，云平台满足应用级灾备切换要求。

10.1.4.2. 数据级灾备测试

数据级灾备主要验证 ISCS（1、2 号线），AFC（2 号线 MLC + ACC），PIS（1、2 号线），ACS（2 号线）的数据级灾备测试，实现方案有如下三种：

1. 方式一：利用备份实现数据灾备
2. 方式二：利用数据库同步软件实现数据库数据级灾备
3. 方式三：利用云平台 CSDR 技术实现数据级灾备
 - 1) 在灾备中心配置数据库的远程容灾
 - 2) 在灾备中心配置这 4 个系统所需最小的计算资源进行配置占位虚机
 - 3) 验证在主用中心不可用的情况下，可手动在灾备中心将这些系统启动，启动后能做到之前所存数据不丢失

注：方式二、方式三需灾备中心增加计算资源（测试时使用虚拟机规格为 4C8G）



数据级灾备网络架构

针对不同业务系统开展不同方案测试，测试结果如下：

1. PIS 数据级灾备（方式一）：

PIS 利用备份软件实现容灾

测试结果：备份软件每天定时将主用中心待备份数据备份至灾备中心，主用中心设备故障，可在灾备中心读取已备份的数据，此方式存在定时备份后至故障时刻时间段内的数据丢失，PIS 业务系统数据重要性相对较低，可容忍此时间段内的数据丢失，通过备份实现 PIS 数据级灾备可满足要求。

2. AFC 数据级灾备（方式二）：

AFC 通过数据库同步软件实现：灾备中心部署虚拟机，通过数据库软件实现主备中心数据库同步

测试结果：数据库同步软件可将主用中心数据库写入的数据实时同步至灾备中心部署的虚拟机，可通过软件读取灾备中心数据库同步的数据。

3. ISCS、ACS 数据级灾备（方式三）：

灾备中心部署虚拟机，通过数据库软件实现主备中心数据库同步

应用虚拟机：利用云平台 CSDR 机制，倒切至灾备中心，实现数据级灾备

测试结果：灾备中心上配置内部网络用于和外部网络及主控中心互联，主用中心故障，灾备中心分配新的资源重新启动服务器，启动可读取虚拟机内部数据，此方式操作较为复杂，实现数据读取在若干小时级别（受数据量大小影响），优点为可通过业务系统软件直接读取历史数据。

注：在数据级灾备场景下，应用系统在灾备中心启动后仅可读取数据，无法对外提供服务

城轨云测试平台测试结果表明云平台可满足城市轨道交通业务系统需求，通过云平台资源灵活调配可提升 50%以上的硬件资源利用率，不仅给城轨云自身的兴建、运营、维护带来显著的经济效益，也为推动城轨云平台行业的信息化智能化标准顺利制定落地实践做出巨大贡献，基于云平台测试平台后续可在此基础上更深入进行：

1. IaaS 层业务系统云化验证：设备虚拟化层次。
2. PaaS 层业务系统云化验证：多业务系统虚拟机融合、跨集群调度协同、多专业数据来源统一、分布式存储。
3. SaaS 层业务系统云化验证：基于大数据的多专业协同的智能调度、智能维保、节能等。
4. 多业务系统上云验证：系统联调与接口测试、多系统融合与共享数据中心相关测试。
5. 主备中心互联测试：网络 SDN 相关测试、安全系统测试、终端相关测试。
6. 更深入进行性能测试和灾备测试。

10.2. IP 地址规划

按照城市轨道交通远期规划战略，在全面研究城市轨道交通线网及线路特性基础上，并结合协会《规范》，为城市轨道交通的 IP 分配提供支持，IP 合理分配是保障轨道交通实现网络信息共享的关键基础工作。IP 规划需考虑既有线路 IP 分配、多线路网络接入、线路延长扩建等因素后，提出满足线网网络需求、适应线路特性、技术先进、安全可靠的 IP 分配方案。

10.2.1. 线路级地址划分

线路级地址规划分为四部分：内部管理网地址、外部服务网地址、安全生产网地址、信号专网地址；

一、内部管理网地址

为内部管理网业务应用系统预留地址；

序号	业务系统	IP 地址段	IP 地址范围	C 段数量	IP 地址数量	路由汇聚
1	车站级企业管理系统	10.21-70.0.0/16	10.21.0.0-10.70.255.255	12800	3276800	10.21-70.0.0/16
2	车站级协同办公系统					
3	其它系统及预留					

二、外部服务网地址

为 CCTV/PBE 业务划分业务地址，预分配每条线 0.5B；

序号	地铁线路	业务系统	IP 地址段	IP 地址范围	C 段数量	IP 地址数量	用途	路由汇聚
1	一号线	视频监控 控系统	10.71.0-73.0/24	10.71.0.0--10.71.73.255	74	18944	CCTV 系统	10.71.0.0/17
		PBE 业 务系统	10.71.74-81.0/24	10.71.74.0--10.71.81.255	8	2048	PBE 业务系 统地址	
		预留	10.71.82-127.0/24	10.71.82.0--10.71.127.255	46	1196	预留	
2	二号线	视频监控 控系统	10.71.128-201.0/24	10.71.128.0--10.71.201.255	74	18944	CCTV 系统	10.71.128.0/17
		PBE 业 务系统	10.71.202-209.0/24	10.71.202.0--10.71.209.255	8	2048	PBE 业务系 统地址	

序号	地铁线路	业务系统	IP 地址段	IP 地址范围	C 段数量	IP 地址数量	用途	路由汇聚
		预留	10.71.210-255.0/24	10.71.210.0--10.71.255.255	46	1196	预留	
3	后 续 线路	预留	10.72-78.0.0/16					

三、安全生产网

安全生产网各业务划分业务 IP 地址，以 1、2 两条线路具体，3-15 号线预留 IP 地址为 10.113-190.0.0/16。

序号	地铁线路	业务系统	IP 地址段	IP 地址范围	C 段数量	IP 地址数量	用途	路由汇聚
1	一 号 线	ISCS 业 务 A 网	10.101.0.0/17	10.101.0.0-10.101.127.255	128	32768	ISCS A 网业务云上服务器	10.101-106.0.0/16
							ISCS 业务 A 网云下设备	
							ISCS A 网云桌面	
		ISCS 业务 B 网	10.102.0.0/17	10.102.0.0-10.102.127.255	128	32768	ISCS B 网云上服务器	
							ISCS 业务 B 网云下设备	
							ISCS B 网云桌面	
		ATS 业 务 A 网	10.101.128.0/17	10.101.128.0-10.101.255.255	128	32768	ATS 业务 A 网云上服务器	
							ATS 业务 A 网云下设备	
							ATS 业务 A 网云桌面	
		ATS 业务 B 网	10.102.128.0/17	10.102.128.0-10.102.255.255	128	32768	ATS 业务 B 网云上服务器	
							ATS 业务 B 网云下设备	
							ATS 业务 B 网云桌面	
		AFC	10.103.0.0/16	10.103.0.0-10.103.	256	65536	AFC 业务系统云上服	

序号	地铁线路	业务系统	IP 地址段	IP 地址范围	C 段数量	IP 地址数量	用途	路由汇聚
		业务系统		255.255			务器	
							AFC 业务系统云下设备	
							AFC 业务系统云桌面	
		PIS 业务系统	10.104.0.0/17	10.104.0.0-10.104.127.255	128	32768	PIS 业务系统云上服务器	
							PIS 业务系统云下设备	
							PIS 业务系统云桌面	
		CAS 业务系统	10.104.128-130.0/24	10.104.128.0-10.104.130.255	3	768	CAS 业务系统云上服务器	
							CAS 集中告警云下接入	
							CAS 业务系统云桌面	
		ACS 业务系统	10.104.131-138.0/24	10.104.131.0-10.104.138.255	8	2048	ACS 系统主中心云上服务器	
							ACS 站段云下设备	
							ACS 业务系统云桌面	
		专用电话	10.104.139.0/24	10.104.139.0-10.104.139.255	1	256	通信系统--专用电话地址	
		LTE 系统	10.104.140-151.0/24	10.104.140.0-10.104.151.255	12	3072	LTE 设备-A 网地址	
							LTE 设备-B 网地址	
							LTE 设备-OM 地址	
		预留	10.104.152-255.0/24	10.104.152.0-10.104.255.255	104	26624	预留	
		宽带集群	10.105.0.0/24	10.105.0.0-10.105.0.255	1	256	宽带集群地址	
		PA 系	10.105.1-3.0/24	10.105.1.0-10.105.	3	768	PA 系统-广播地址	

序号	地铁线路	业务系统	IP 地址段	IP 地址范围	C 段数量	IP 地址数量	用途	路由汇聚
		统 - 广播		3.255				
		CLK 系统	10.105.4.0/24	10.105.4.0-10.105.4.255	1	256	CLK 时钟系统地址	
		专 用 通 信 系统-- 传输	10.105.5-44.0/24	10.105.5.0-10.105.44.255	40	10240	专用通信--传输系统地址	
		集 中 录音	10.105.45.0/24	10.105.45.0-10.105.45.255	1	256	专用通信--集中录音系统	
		专 用 通 信 系统-- 电源	10.105.46.0/24	10.105.46.0-10.105.46.255	1	256	主中心、主中心监控网管	
		预留	10.105.47-50.0/24	10.105.47.0-10.105.50.255	4	1024	预留	
		杂 散 电 流 系统	10.105.51.0/24	10.105.51.0-10.105.51.255	1	256	牵引变电所监测装置	
		UPS 电 源 系统	10.105.52.0/24	10.105.52.0-10.105.52.255	1	256	电源网管设备/电源监控主机	
		可 视 化 接 地 系 统	10.105.53.0/24	10.105.53.0-10.105.53.255	1	256	牵引变电所监控装置	
		PCM 系统	10.105.54.0/24	10.105.54.0-10.105.54.255	1	256	PCM 系统	
		再 生 制 动 能 量 回 馈	10.105.55.0/24	10.105.55.0-10.105.55.255	1	256	再生制动能量回馈装置系统	

序号	地铁线路	业务系统	IP 地址段	IP 地址范围	C 段数量	IP 地址数量	用途	路由汇聚
		装 置 系统						
		PSCD A	10.105.56.0/24	10.105.56.0-10.10 5.56.255	1	256	PSCDA	
		FAS	10.105.57.0/24	10.105.57.0-10.10 5.57.255	1	256	FAS	
		预留	10.105.58-59.0/24	10.105.58.0-10.10 5.59.255	2	512	预留	
		公 安 通 信 系 统 中 的 传 输	10.105.60-61.0/24	10.105.60.0-10.10 5.61.255	2	512	公安通信传输系统地址	
		公 安 计 算 机 网 络	10.105.62-65.0/24	10.105.62.0-10.10 5.65.255	4	1024		
		公 安 电 源 系统	10.105.66.0/24	10.105.66.0-10.10 5.66.255	1	256		
		公 安 无 线	10.105.67-68.0/24	10.105.67.0-10.10 5.68.255	2	512		
		预留	10.105.69.0/24	10.105.69.0-10.10 5.69.255	1	256	预留	
		列 车 在 线 检 测 装置	10.105.70.0/24	10.105.70.0-10.10 5.70.255	1	256		
		安 全 联 锁 装置						

序号	地铁线路	业务系统	IP 地址段	IP 地址范围	C 段数量	IP 地址数量	用途	路由汇聚
		自动化立体仓储设备						
		车辆段工艺/厨房设备	10.105.71.0/24	10.105.71.0-10.105.71.255	1	256		
		预留	10.105.72-79.0/24	10.105.72.0-10.105.79.255	8	2048	预留	
		安检系统	10.105.80-81.0/24	10.105.80.0-10.105.81.255	2	512	站段安检设备 X 光机、安检门、工作站、各类交换机、各类控制器或服务器等	
		车场安防系统	10.105.82-101.0/24	10.105.82.0-10.105.101.255	20	5120	场段中安防系统中的广播、视频、出入口控制系统等	
		预留	10.105.102-255.0/24	10.105.102.0-10.105.255.255	154	39424	预留	
		预留	10.106.0.0/16	10.106.0.0-10.106.255.255	256	65536	预留	
2	二号线	ISCS 业务 A 网	10.107.0.0/17	10.107.0.0-10.107.127.255	128	32768	ISCS A 网云上服务器	10.107-112.0.0/16
							ISCS 业务 A 网云下设备	
							ISCS A 网云桌面地址	
		ISCS 业务 B 网	10.108.0.0/17	10.108.0.0-10.108.127.255	128	32768	ISCS B 网云上服务器	
							ISCS 业务 B 网云下设备	
							ISCS B 网云桌面地址	

序号	地铁线路	业务系统	IP 地址段	IP 地址范围	C 段数量	IP 地址数量	用途	路由汇聚
		ATS 业务 A 网	10.107.128.0/17	10.107.128.0-10.107.255.255	128	32768	ATS 业务 A 网云上服务器	
							ATS 业务 A 网云下设备	
							ATS 业务 A 网云桌面地址	
		ATS 业务 B 网	10.108.128.0/17	10.108.128.0-10.108.255.255	128	32768	ATS 业务 B 网云上服务器	
							ATS 业务 B 网云下设备	
							ATS 业务 B 网云桌面地址	
		AFC 业务系统	10.109.0.0/16	10.109.0.0-10.109.255.255	256	65536	AFC 业务系统云上服务器	
							AFC 业务系统云下设备	
							AFC 业务系统云桌面	
		PIS 业务系统	10.110.0.0/17	10.110.0.0-10.110.127.255	128	32768	PIS 业务系统云上服务器	
							PIS 业务系统云下设备	
							PIS 业务系统云桌面	
		CAS 业务系统	10.110.128-130.0/24	10.110.128.0-10.110.130.255	3	768	CAS 业务系统云上服务器	
							CAS 集中告警云下设备	
							CAS 业务系统云桌面	
		ACS 业务	10.110.131-138.0/24	10.110.131.0-10.110.138.255	8	2048	ACS 系统云上服务器	
							ACS 站段云下设备	

序号	地铁线路	业务系统	IP 地址段	IP 地址范围	C 段数量	IP 地址数量	用途	路由汇聚
		系统					ACS 业务系统云桌面地址	
		专 用 电话	10.110.139.0/24	10.110.139.0-10.1 10.139.255	1	256	通信系统--专用电话地址	
		LTE 系统	10.110.140-151.0/24	10.110.140.0-10.1 10.151.255	12	3072	LTE 设备-A 网地址	
							LTE 设备-B 网地址	
							LTE 设备-OM 地址	
		预留	10.110.152-255.0/24	10.110.152.0-10.1 10.255.255	104	26624	预留	
		宽 带 集群	10.111.0.0/24	10.111.0.0-10.111. 0.255	1	256	宽带集群地址	
		PA 系 统 - 广 播	10.111.1-3.0/24	10.111.1.0-10.111. 3.255	3	768	PA 系统-广播地址	
		CLK 系统	10.111.4.0/24	10.111.4.0-10.111. 4.255	1	256	CLK 时钟系统地址	
		专 用 通 信 系统-- 传输	10.111.5-44.0/24	10.111.5.0-10.111. 44.255	40	10240	专用通信--传输系统地址	
		集 中 录音	10.111.45.0/24	10.111.45.0-10.11 1.45.255	1	256	专用通信--集中录音系统	
		专 用 通 信 系统-- 电源	10.111.46.0/24	10.111.46.0-10.11 1.46.255	1	256	主中心、主中心监控网管	
		预留	10.111.47-50.0/24	10.111.47.0-10.11 1.50.255	4	1024	预留	
		杂 散 电 流	10.111.51.0/24	10.111.51.0-10.11 1.51.255	1	256	牵引变电所监测装置	

序号	地铁线路	业务系统	IP 地址段	IP 地址范围	C 段数量	IP 地址数量	用途	路由汇聚
		系统						
		UPS 电 源 系统	10.111.52.0/24	10.111.52.0-10.11 1.52.255	1	256	电源网管设备/电源监 控主机	
		可 视 化 接 地 系 统	10.111.53.0/24	10.111.53.0-10.11 1.53.255	1	256	牵引变电所监控装置	
		PCM 系统	10.111.54.0/24	10.111.54.0-10.11 1.54.255	1	256	PCM 系统	
		再 生 制 动 能 量 回 馈 装 置 系统	10.111.55.0/24	10.111.55.0-10.11 1.55.255	1	256	再生制动能量回馈装 置系统	
		PSCD A	10.111.56.0/24	10.111.56.0-10.11 1.56.255	1	256	PSCDA	
		FAS	10.111.57.0/24	10.111.57.0-10.11 1.57.255	1	256	FAS	
		预留	10.111.58-59.0/24	10.111.58.0-10.11 1.59.255	2	512	预留	
		公 安 通 信 系 统 中 的 传 输	10.111.60-61.0/24	10.111.60.0-10.11 1.61.255	2	512	公安通信传输系统地 址	
		公 安 计 算 机 网 络	10.111.62-65.0/24	10.111.62.0-10.11 1.65.255	4	1024	/	
		公 安	10.111.66.0/24	10.111.66.0-10.11	1	256	/	

序号	地铁线路	业务系统	IP 地址段	IP 地址范围	C 段数量	IP 地址数量	用途	路由汇聚
		电 源系统		1.66.255				
		公 安无线	10.111.67-68.0/24	10.111.67.0-10.111.68.255	2	512	/	
		预留	10.111.69.0/24	10.111.69.0-10.111.69.255	1	256	预留	
		列 车在线检测装置	10.111.70.0/24	10.111.70.0-10.111.70.255	1	256	/	
		安 全联锁装置						
		自 动化立体仓储设备						
		车 辆段工艺/厨房设备	10.111.71.0/24	10.111.71.0-10.111.71.255	1	256	/	
		预留	10.111.72-79.0/24	10.111.72.0-10.111.79.255	8	2048	预留	
		安 检系统	10.111.80-81.0/24	10.111.80.0-10.111.81.255	2	512	站段安检设备 X 光机、安检门、工作站、各类交换机、各类控制器或服务器等	
		车 场安防系统	10.111.82-101.0/24	10.111.82.0-10.111.101.255	20	5120	场段中安防系统中的广播、视频、出入口控制系统等	

序号	地铁线路	业务系统	IP 地址段	IP 地址范围	C 段数量	IP 地址数量	用途	路由汇聚
		预留	10.111.102-255.0/24	10.111.102.0-10.111.255.255	154	39424	预留，新业务等	
		预留	10.112.0.0/16	10.112.0.0-10.112.255.255	256	65536	预留，新业务等	

四、信号专网

为信号专网预留每条线 1B 的地址；

序号	地铁线路	IP 地址段	IP 地址范围	C 段数量	IP 地址数量	路由汇聚
1	一号线	10.201.0.0/16	10.201.0.0-10.201.255.255	256	65536	10.201-215.0.0/16
2	二号线	10.202.0.0/16	10.202.0.0-10.202.255.255	256	65536	
3	三号线	10.203.0.0/16	10.203.0.0-10.203.255.255	256	65536	
4	四号线	10.204.0.0/16	10.204.0.0-10.204.255.255	256	65536	
5	五号线	10.205.0.0/16	10.205.0.0-10.205.255.255	256	65536	
6	六号线	10.206.0.0/16	10.206.0.0-10.206.255.255	256	65536	
7	七号线	10.207.0.0/16	10.207.0.0-10.207.255.255	256	65536	
8	八号线	10.208.0.0/16	10.208.0.0-10.208.255.255	256	65536	
9	九号线	10.209.0.0/16	10.209.0.0-10.209.255.255	256	65536	
10	十号线	10.210.0.0/16	10.210.0.0-10.210.255.255	256	65536	
11	十一号线	10.211.0.0/16	10.211.0.0-10.211.255.255	256	65536	
12	十二号线	10.212.0.0/16	10.212.0.0-10.212.255.255	256	65536	
13	十三号线	10.213.0.0/16	10.213.0.0-10.213.255.255	256	65536	
14	十四号线	10.214.0.0/16	10.214.0.0-10.214.255.255	256	65536	
15	十五号线	10.215.0.0/16	10.215.0.0-10.215.255.255	256	65536	
16	预留线路	10.216-250.0.0/16	10.215.0.0-10.250.255.255	8960	2293760	10.216-250.0.0/16

10.2.2. 线网级地址划分

线网级地址划分为安全生产网地址、内部管理网地址、外部服务网地址。每网均是按照业务系统划分大的网段，不再分到具体每条线；

一、安全生产网

为安生生产网的 PIS、AFC 分配的地址及预留；

序号	业务系统	IP 地址段	IP 地址范围	C 段数量	IP 地址数量	用途	路由汇聚
1	PIS	172.16.0.0/24	172.16.0.0-172.16.0.255	1	256	PIS（1-15 号线）	172.16-21.0.0/16
2	AFC	172.16.1-12.0/24	172.16.1.0-172.16.12.255	12	3072	AFC 清分系统、MLC 系统（1-15 号线）	
3	数据挖掘	172.16.13.0/24	172.16.13.0-172.16.13.255	1	256	数据挖掘	
4	预留	172.16.14-255.0/24	172.16.14.0-172.16.255.255	242	61952	预留	
5	预留	172.17-21.0.0/16	172.17.0.0-172.21.255.255	1280	327680	预留	

二、内部管理网

为 OA 分配的地址及预留；

序号	业务系统	IP 地址段	IP 地址范围	C 段数量	IP 地址数量	用途	路由汇聚
1	企业管理系统	172.22.0-19.0/24	172.22.0.0-172.22.19.255	20	5120	OA 办公自动化等	172.22-23.0.0/16
2	预留	172.22.20-255.0/24	172.22.20.0-172.22.255.255	236	60416	预留	
3	数据挖掘	172.23.0.0/24	172.23.0.0-172.23.0.255	1	256	数据挖掘	
4	预留	172.23.1.0/16	172.23.1.0-172.23.255.255	255	65280	预留	

三、外部服务网

为 CCTV、PBE、AFC 分配的地址及预留；

序号	业务系统	IP 地址段	IP 地址范围	C 段数量	IP 地址数量	用途	路由汇聚
1	视频监控系	172.24.0.0/24	172.24.0.0-172.24.0.255	1	256	CCTV 业务系	172.24-29.0.0/16

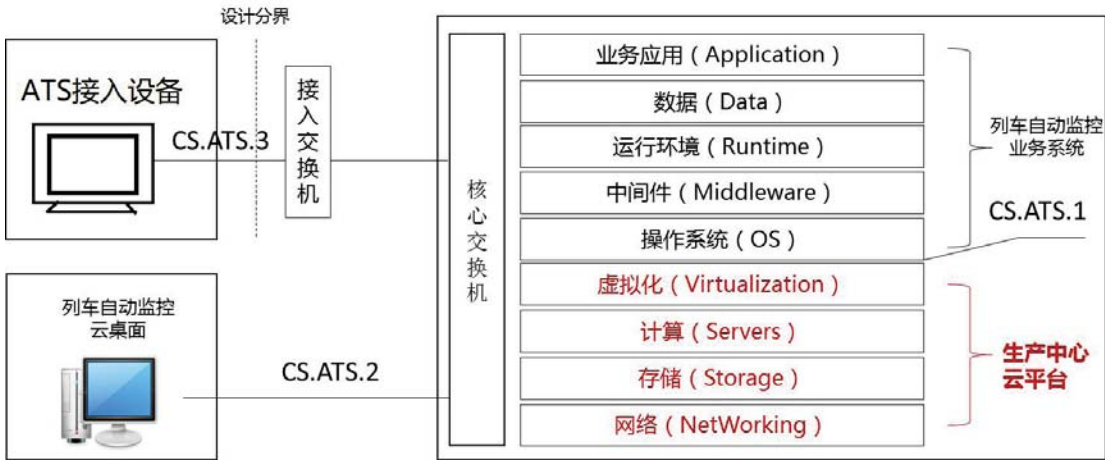
序号	业务系统	IP 地址段	IP 地址范围	C 段数量	IP 地址数量	用途	路由汇聚
	统					统地址	
2	PBE 系统	172.24.1-3.0/24	172.24.1.0-172.24.3.255	3	768	PBE 业务系统地址	
3	互联网售票	172.24.4-6.0/24	172.24.4.0-172.24.6.255	3	768	AFC 业务系统地址	
4	OA	172.24.7-8.0/24	172.24.7.0-172.24.8.255	2	512	公司网站、邮箱等	
5	预留	172.24.9-255.0/24	172.24.9.0-172.24.255.255	247	63232	预留	
6	预留	172.25-29.0.0/24	172.25.0.0-172.29.255.255	1280	327680	预留	

10.3. 接口技术要求

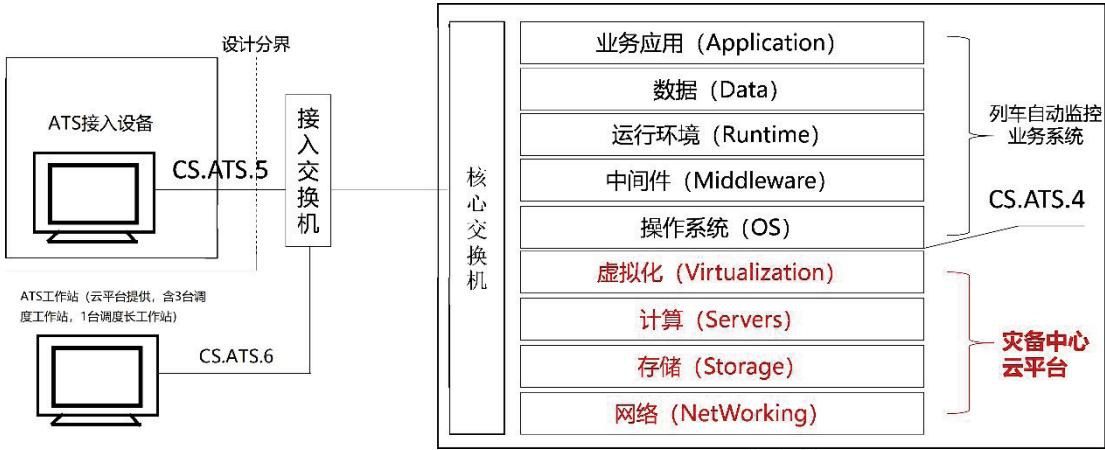
10.3.1.接口界面

10.3.1.1 云平台与 ATS 接口界面及功能要求

1、生产中心云平台与 ATS 接口界面划分示意图：



2、灾备中心云平台与 ATS 界面划分示意图：



3、虚拟接口

编号	位置	CS	ATS	接口类型	备注
CS.ATS.1	生产中心云平台专用机房	提供虚拟服务器、网络及存储；负责	提供操作系统、数据库软件、应用软件、业务系统安全软件；负责业	接口在中心云平台 IaaS 层	

编号	位置	CS	ATS	接口类型	备注
		云平台性能调试。	务性能调试。		
CS.ATS.2	生产中心 ATS 设置云桌面的房间	提供云桌面；提供瘦客户端（含显示器、键鼠）；负责云平台性能调试。	提供操作系统、数据库软件、应用软件、业务系统安全软件；负责业务性能调试。	接口在中心云桌面侧	
CS.ATS.4	灾备中心云平台专用机房	提供虚拟服务器、网络及存储；负责云平台性能调试。	提供操作系统、数据库软件、应用软件、业务系统安全软件；负责业务性能调试。	接口在中心云平台 IaaS 层	

4、物理接口

编号	位置	云平台	ATS	接口类型	备注
CS.ATS.3	生产中心云平台配线间	负责云平台侧调试及云平台端光缆上架	负责连接至 1 号线信号设备室配线架外侧；负责业务侧调试	2 个冗余的 1000M 单模光口，LC	线缆由控制中心施工单位提供并实施。线缆成端由各专业施工单位实施 两光口互为冗余
CS.ATS.5	灾备中心云平台配线间	负责云平台侧调试及云平台端光缆上架	负责连接至 1 号线信号设备室配线架外侧；负责业务侧调试	2 个冗余的 1000M 单模光口，LC	线缆由控制中心施工单位提供并实施。线缆成端由各专业施工单位实施 两光口互为冗余
CS.ATS.6	灾备中心	提供 4 台 ATS 工作站物理设备（含键盘鼠标、显示器）；	负责业务调试	每台设备 2 个 1000M 以太网光口或 RJ45	线缆由云平台施工单位提供并实施

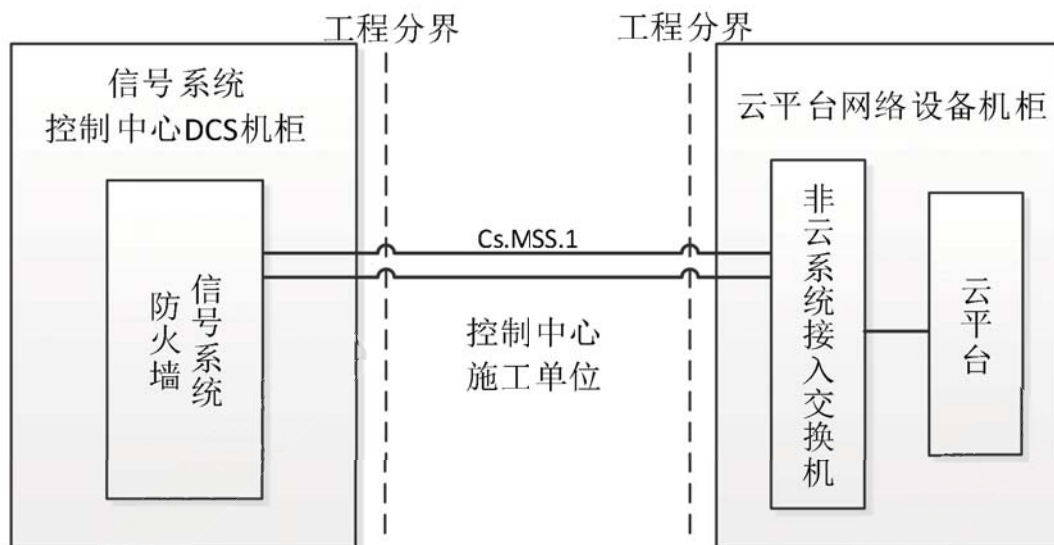
编号	位置	云平台	ATS	接口类型	备注
		负责将设备连入灾备中心云平台业务接入交换机			

5、功能要求

编号	功能要求	云平台	ATS	备注
CS.ATS.1	在生产中心提供列车自动监控业务服务	提供虚拟服务器、网络及存储	提供操作系统、数据库软件、应用软件、系统安全软件	
CS.ATS.2	在生产中心列车自动监控桌面云终端与云平台间建立信息传输通道	提供桌面云终端、桌面云服务	提供操作系统、客户端软件、系统安全软件	
CS.ATS.3	在生产中心 ATS 防火墙物理设备与云平台间建立信息传输通道	提供网络	提供物理设备及自身配套软件	
CS.ATS.4	在灾备中心提供列车自动监控业务服务	提供虚拟服务器、网络及存储	提供操作系统、数据库软件、应用软件、系统安全软件	
CS.ATS.5	在灾备中心 ATS 防火墙物理设备与云平台间建立信息传输通道	提供网络	提供物理设备及自身配套软件	
CS.ATS.6	在灾备中心提供列车自动监控业务的工作站	提供 4 台 ATS 工作站及其网络、供电	提供操作系统、数据库软件、应用软件、系统安全软件	

10.3.1.2 云平台与 MSS 接口界面及功能要求

1、生产中心云平台与 MSS 接口界面划分示意图：



2、接口位置

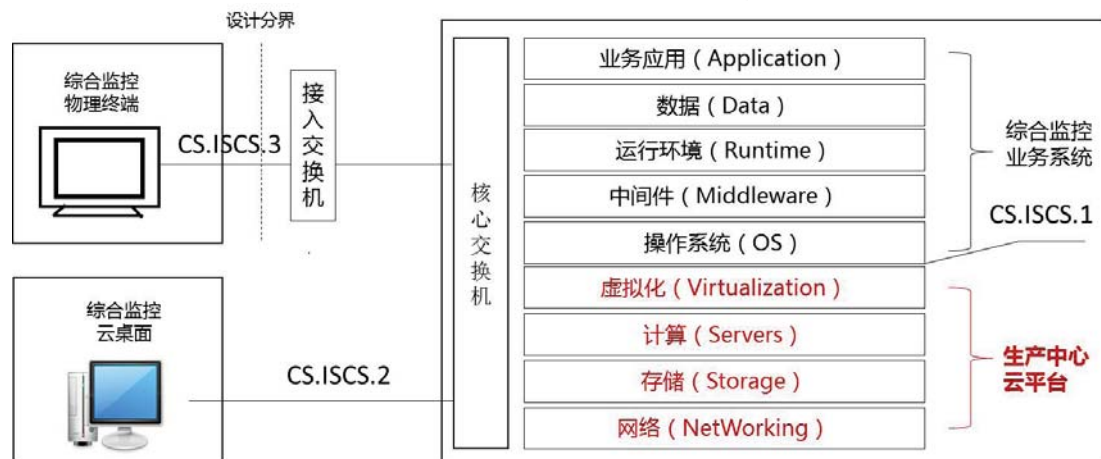
编号	位置	云平台	MSS	接口类型	备注
CS.MSS.1	生产中心云平台各层配线间	负责云平台侧调试及云平台端光缆上架	负责连接至控制中心2号线信号设备室配线架外侧；负责业务侧调试	1 个 1000M 单模光口，LC	线缆由控制中心施工单位提供并实施。线缆成端由各专业施工单位实施

3、功能要求

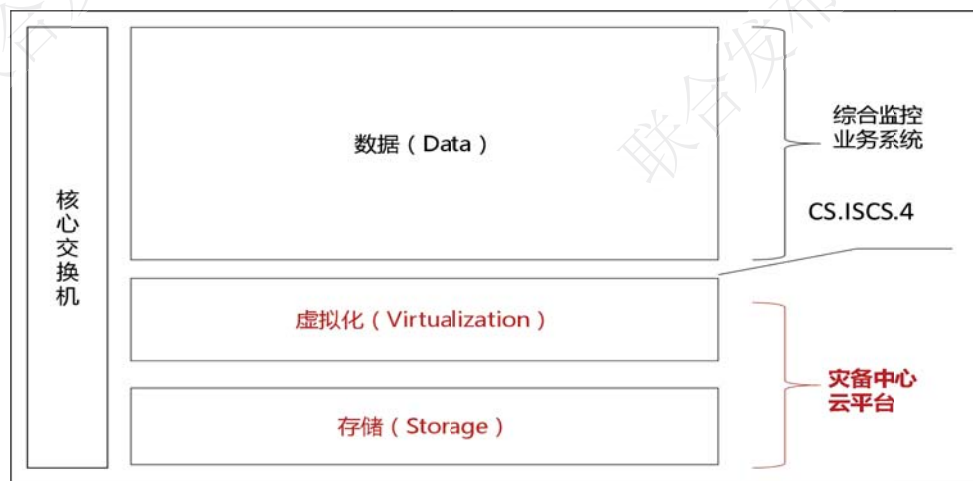
编号	功能要求	云平台	MSS	备注
CS.MSS.1	为实现云平台数据挖掘功能	搭建数据挖掘平台,通过算法、模型等完成数据挖掘相关工作。	在生产中心提供信号系统设备维护等信息	数据详细内容待定。

10.3.1.3 云平台与 ISCS 接口界面及功能要求

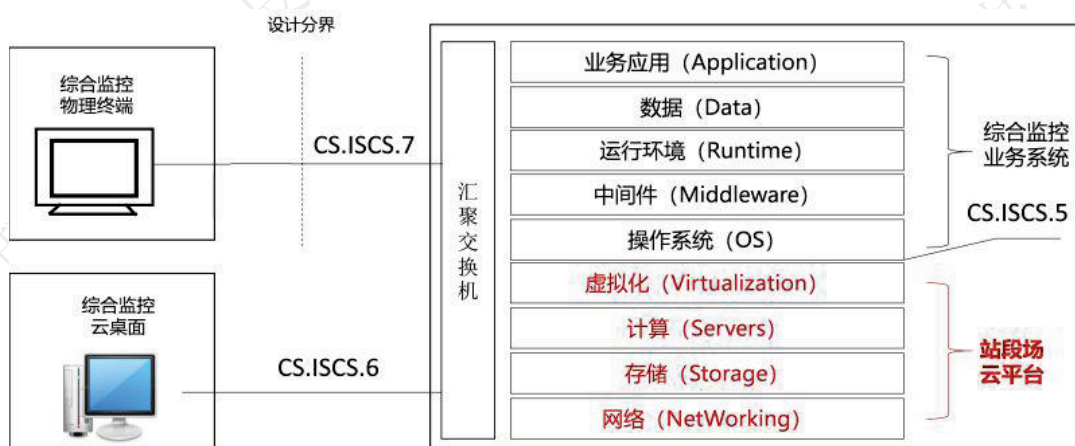
1、生产中心云平台与 ISCS 界面划分示意图：



2、灾备中心云平台与 ISCS 界面划分示意图：



3、站段场云平台与 ISCS 界面划分示意图：



4、虚拟接口

编号	位置	CS	ISCS	接口类型	备注
----	----	----	------	------	----

编号	位置	CS	ISCS	接口类型	备注
CS.ISCS.1	生产中心云平台专用机房	提供虚拟服务器、网络及存储；负责云平台性能调试。	提供操作系统、数据库软件、应用软件、业务系统安全软件；负责业务性能调试。	接口在中心云平台 IaaS 层	
CS.ISCS.2	生产中心综合监控设置云桌面的房间	提供云桌面；提供瘦客户端（含显示器、键鼠）；负责云平台性能调试。	提供操作系统、数据库软件、应用软件、业务系统安全软件；负责业务性能调试。	接口在中心云桌面侧	
CS.ISCS.5	站段场弱电综合机房	提供虚拟服务器、网络及存储；负责云平台性能调试。	提供操作系统、数据库软件、应用软件、业务系统安全软件；负责调试。	接口在站段场云平台 IaaS 层	
CS.ISCS.6	站段场综合监控设置云桌面的房间	提供云桌面；提供瘦客户端（含显示器、键鼠）；负责云平台性能调试。	提供操作系统、数据库软件、应用软件、业务系统安全软件；负责业务性能调试。	接口在车站云桌面侧	

5、物理接口

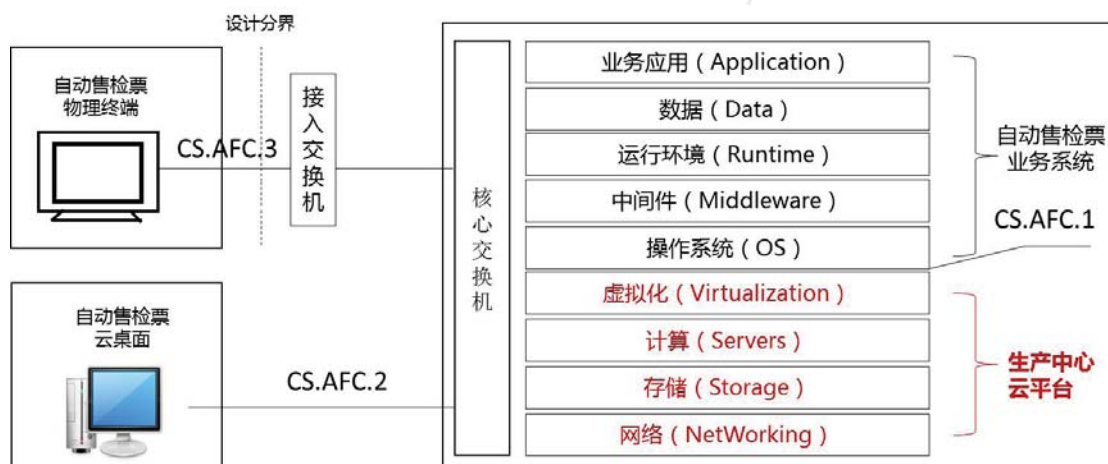
编号	位置	云平台	ISCS	接口类型	备注
CS.ISCS.3	生产中心云平台各层配线间或生产中心云平台业务接入交换机	负责云平台侧调试	负责将非云物理设备连接至中心各层配线间云平台综合配线架外线侧；负责业务侧调试	2 个冗余的 1000M 以太网单模光口	
CS.ISCS.7	站段场弱电综合机房的站段交换机	负责云平台侧调试	负责将 ISCS 站段场交换机连接至站段场云平台配线架外线侧；负责业务侧调试	2 个冗余的 1000M 以太网单模光口	

6、功能要求

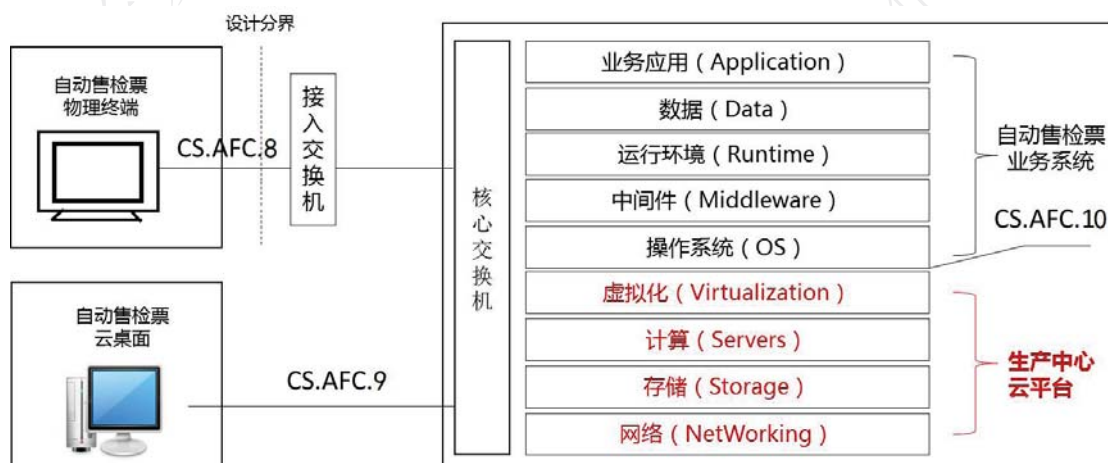
编号	功能要求	云平台	ISCS	备注
CS.ISCS.1	在生产中心提供综合监控业务服务	提供虚拟服务器、网络及存储	提供操作系统、数据库软件、应用软件、系统安全软件	
CS.ISCS.2	在生产中心综合监控桌面云终端与云平台间建立信息传输通道	提供桌面云终端、桌面云服务	提供操作系统、客户端软件、系统安全软件	
CS.ISCS.3	在生产中心综合监控物理设备与云平台间建立信息传输通道	提供网络	提供连接线缆，自身配套软件	
CS.ISCS.4	在灾备中心提供综合监控业务服务	提供存储	提供业务数据等	
CS.ISCS.5	在站段场提供综合监控业务服务	提供虚拟服务器、网络及存储	提供操作系统、数据库软件、应用软件、系统安全软件	
CS.ISCS.6	在站段场综合监控桌面云终端与云平台间建立信息传输通道	提供桌面云终端、桌面云服务	提供操作系统、客户端软件、系统安全软件	
CS.ISCS.7	在站段场综合监控物理设备与云平台间建立信息传输通道	提供网络	提供连接线缆及自身配套软件	

10.3.1.4 云平台与 ACC 接口界面及功能要求

1、生产中心云平台与 ACC 界面划分示意图：



2、生产中心云平台与 ACC 测试中心系统界面划分示意图：



3、虚拟接口

编号	位置	CS	ACC	接口类型	备注
CS.AFC.1	生产中心云平台专用机房	提供虚拟服务器、网络及存储；负责云平台性能调试。	提供操作系统、数据库软件、应用软件、业务系统安全软件；负责业务性能调试。	接口在中心云平台 IaaS 层	
CS.AFC.2	生产中心 ACC 设置云桌面的房间	提供云桌面；提供瘦客户端（含显示器、键鼠）；负责云平台性能调试。	提供操作系统、数据库软件、应用软件、业务系统安全软件；负责业务性能调试。	接口在中心云桌面侧	
CS.AFC.9	生产中心 ACC 测试中心系统设置云桌面的	提供云桌面；提供瘦客户端（含显示器、键鼠）；负责云平台	提供操作系统、数据库软件、应用软件、业务系统安全软件；	接口在中心测试云桌面侧	

编号	位置	CS	ACC	接口类型	备注
	房间	性能调试。	负责业务性能调试。		
CS.AFC.10	生产中心云平台专用机房	提供虚拟服务器、网络及存储；负责云平台性能调试。	提供操作系统、数据库软件、应用软件、业务系统安全软件；负责业务性能调试。	接口在中心云平台 IaaS 层	

4、物理接口

编号	位置	云平台	ACC	接口类型	备注
CS.AFC.3	生产中心云平台各层配线间的 ODF 配线架	负责云平台侧调试	负责将非云物理设备连接至中心各层配线间云平台综合配线架外线侧；负责业务侧调试	2 个冗余的 1000M 单模光口，LC	线缆由 ACC 施工单位提供并实施
CS.AFC.8	生产中心云平台各层配线间的 ODF 配线架	负责云平台侧调试	负责将非云物理设备连接至中心各层配线间云平台综合配线架外线侧；负责业务侧调试	2 个冗余的 1000M 单模光口，LC	线缆由 ACC 施工单位提供并实施

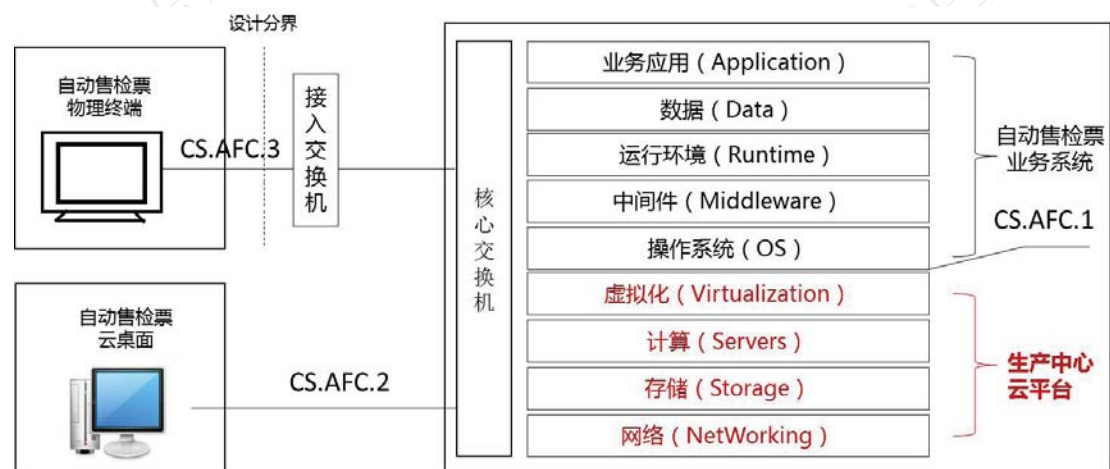
5、功能要求

编号	功能要求	云平台	ISCS	备注
CS.AFC.1	在生产中心提供自动售检票业务服务	提供虚拟服务器、网络及存储	提供操作系统、数据库软件、应用软件、系统安全软件	
CS.AFC.2	在生产中心自动售检票桌面云终端与云平台间建立信息传输通道	提供桌面云终端、桌面云服务	提供操作系统、客户端软件、系统安全软件	
CS.AFC.3	在生产中心自动售检票物理设备与云平台间建立信息传输通道	提供网络、安全	提供物理终端、服务软件、系统安全软件	
CS.AFC.8	在生产中心自动售检票测试中心系统物理设备与云平台间建立信息传输通道	提供网络、安全	提供物理终端、服务软件、系统安全软件	

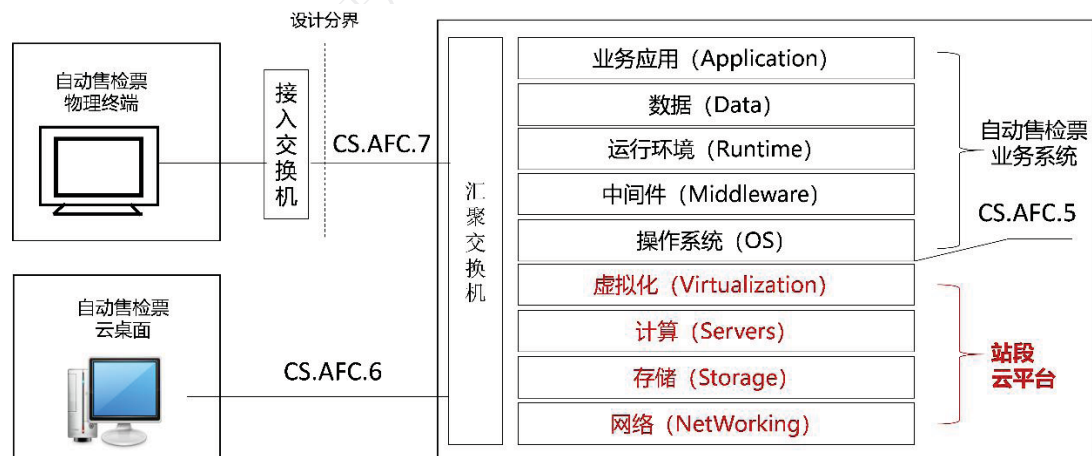
CS.AFC.9	在生产中心自动售检票测试中心系统桌面云终端与云平台间建立信息传输通道	提供桌面云终端、桌面云服务	提供操作系统、客户端软件、系统安全软件	
CS.AFC.10	在生产中心提供自动售检票业务服务	提供虚拟服务器、网络及存储	提供操作系统、数据库软件、应用软件、系统安全软件	

10.3.1.5 云平台与 MLC 接口界面及功能要求

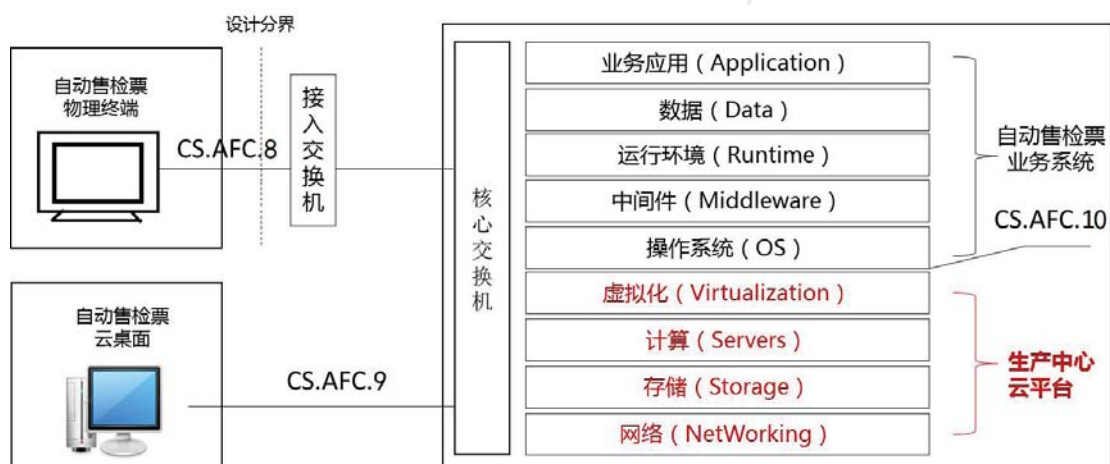
1、生产中心云平台与 AFC 界面划分示意图：



2、车站云平台与 AFC 界面划分示意图：



3、生产中心云平台与 AFC 测试中心系统界面划分示意图：



4、虚拟接口

编号	位置	CS	AFC	接口类型	备注
CS.AFC.1	生产中心云平台专用机房	提供虚拟服务器、网络及存储；负责云平台性能调试。	提供操作系统、数据库软件、应用软件、业务系统安全软件；负责业务性能调试。	接口在中心云平台 IaaS 层	
CS.AFC.2	生产中心 AFC 设置云桌面的房间	提供云桌面；提供瘦客户端（含显示器、键鼠）；负责云平台性能调试。	提供操作系统、数据库软件、应用软件、业务系统安全软件；负责业务性能调试。	接口在中心云桌面侧	
CS.AFC.5	站段弱电综合机房	提供虚拟服务器、网络及存储；负责云平台性能调试。	提供操作系统、数据库软件、应用软件、业务系统安全软件；负责业务性能调试。	接口在站段云平台 IaaS 层	
CS.AFC.6	站段自动售检票设置云桌面的房间	提供云桌面；提供瘦客户端（含显示器、键鼠）；负责云平台性能调试。	提供操作系统、数据库软件、应用软件、业务系统安全软件；负责业务性能调试。	接口在站段云桌面侧	
CS.AFC.9	生产中心 AFC 测试中心系统设置云桌面的房间	提供云桌面；提供瘦客户端（含显示器、键鼠）；负责云平台性能调试。	提供操作系统、数据库软件、应用软件、业务系统安全软件；负责业务性能调试。	接口在中心测试云桌面侧	

编号	位置	CS	AFC	接口类型	备注
CS.AFC.10	生产中心云平台专用机房	提供虚拟服务器、网络及存储；负责云平台性能调试。	提供操作系统、数据库软件、应用软件、业务系统安全软件；负责业务性能调试。	接口在中心云平台 IaaS 层	

5、物理接口

编号	位置	云平台	AFC	接口类型	备注
CS.AFC.3	生产中心云平台各层配线间的 ODF 配线架	负责云平台侧调试	负责将非云物理设备连接至中心各层配线间云平台综合配线架外线侧；负责业务侧调试	2 个冗余的 1000M 单模光口，LC	线缆由 AFC 施工单位提供并实施
CS.AFC.7	站段弱电综合机房的站段交换机	负责云平台侧调试	负责将 AFC 站段交换机连接至车站云平台配线架外线侧；负责业务侧调试	2 个冗余的 1000M 单模光口，LC	线缆由 AFC 施工单位提供并实施
CS.AFC.8	生产中心云平台各层配线间的 ODF 配线架	负责云平台侧调试	负责将非云物理设备连接至中心各层配线间云平台综合配线架外线侧；负责业务侧调试	2 个冗余的 1000M 单模光口，LC	线缆由 AFC 施工单位提供并实施

6、功能要求

编号	功能要求	云平台	AFC	备注
CS.AFC.1	在生产中心提供自动售检票业务服务	提供虚拟服务器、网络及存储	提供操作系统、数据库软件、应用软件、系统安全软件	
CS.AFC.2	在生产中心自动售检票桌面云终端与云平台间建立信息传输通道	提供桌面云终端、桌面云服务	提供操作系统、客户端软件、系统安全软件	
CS.AFC.3	在生产中心自动售检票物理设备与云平台	提供网络、安全	提供物理终端、服务软件、系统安全软件	

	间建立信息传输通道			
CS.AFC.5	在车站提供自动售检票业务服务	提供虚拟服务器、网络及存储	提供操作系统、数据库软件、应用软件、系统安全软件	
CS.AFC.6	在车站自动售检票桌面云终端与云平台间建立信息传输通道	提供桌面云终端、桌面云服务	提供操作系统、客户端软件、系统安全软件	
CS.AFC.7	在站段自动售检票物理设备与云平台间建立信息传输通道	提供网络	提供物理终端、服务软件、系统安全软件	
CS.AFC.8	在生产中心自动售检票测试中心系统物理设备与云平台间建立信息传输通道	提供网络、安全	提供物理终端、服务软件、系统安全软件	
CS.AFC.9	在生产中心自动售检票测试中心系统桌面云终端与云平台间建立信息传输通道	提供桌面云终端、桌面云服务	提供操作系统、客户端软件、系统安全软件	
CS.AFC.10	在生产中心提供自动售检票业务服务	提供虚拟服务器、网络及存储	提供操作系统、数据库软件、应用软件、系统安全软件	

10.3.2. 测试分工

1. 测试工作需要业务系统供货商与云平台系统供货商相互配合完成及共同确认；
2. 云平台系统供货商向甲方提交测试计划和测试报告业务系统供货商配合云平台完成测试计划和测试报告；
3. 测试的内容包括下表所示之内容：

测试类别		目的	测试阶段
连接	目视测试	检查各接口是否恰当地、正确地接连到双方指定的端点上。	系统安装
	点对点测试	检查各接口是否恰当地、正确地连接。	系统安装

测试类别		目的	测试阶段
测试	端对端测试	检查各接口端对端是否恰当地、正确地连接。	系统安装
	通信测试	测试各接口双方的通电连续性 & 数据连接状态。	系统安装
承载测试	兼容性测试	验证业务系统能在云平台上可靠地运行	接口测试
	功能测试	验证业务系统功能实现	接口测试
	性能测试	验证云平台提供的资源满足业务系统业务性能需求	现场单调验证

10.4. 参与单位及主要技术人员名单

专业	参与单位	主要技术人员
建设单位	呼和浩特市城市轨道交通建设管理有限公司	吕 涛
建设单位	呼和浩特市城市轨道交通建设管理有限公司	胡晓伟
建设单位	呼和浩特市城市轨道交通建设管理有限公司	孟 飞
建设单位	呼和浩特市城市轨道交通建设管理有限公司	刘 芽
建设单位	呼和浩特市城市轨道交通建设管理有限公司	李正浩
建设单位	呼和浩特市城市轨道交通建设管理有限公司	张斯嘉
运营单位	呼和浩特地铁运营有限公司	任 福
运营单位	呼和浩特地铁运营有限公司	郭旭东
运维单位	内蒙古交控安捷科技有限公司	徐文升
运维单位	内蒙古交控安捷科技有限公司	宿建伟
设计单位	中国铁路设计集团有限公司	冯 璐
设计单位	中国铁路设计集团有限公司	周建美
设计单位	中国铁路设计集团有限公司	霍文荟
设计单位	中国铁路设计集团有限公司	王奕凯
云平台	交控科技股份有限公司	毛新德
云平台	交控科技股份有限公司	赵辰兵
云平台	交控科技股份有限公司	周驰楠
云平台	交控科技股份有限公司	付 宇
云平台	交控科技股份有限公司	狄金山