

doi: 10.3969/j.issn.1672-6073.2020.05.001

编者按 2016年初,中国城市轨道交通协会专家和学术委提出我国城轨信息化“13531”的发展蓝图,首次在城轨行业提出搭建一个“城市轨道交通云平台”的理念,开启城轨云研究应用的征程。2019年12月,首部基于城轨云的规范正式实施,开创了城轨交通信息化规范化建设、标准化运营的历史,填补了城轨交通信息化专业标准的空白。2019年底,呼和浩特市首条地铁线路开通试运营,标志着中国标准城轨云在城市轨道交通中成功应用,2020年3月,《智慧城轨发展纲要》的发布以及逐步实行的“1352(1个总体规范,3个技术规范,5个关键技术规范,2个实用技术规范)”城轨云技术规范体系,得到了业界的普遍认可和广泛应用,取得了良好的效果。城轨云建设跨入世界前列。

近期,为贯彻落实《智慧城轨发展纲要》,研究应用城轨云技术,本刊开展了以城轨云和网络安全为热点的学术研讨,征集并精选了6篇论文,旨在以城轨云的创新研究和成功实践,助推智慧城轨建设,开创中国城轨高质量发展的新局面。

以云平台为底座的城轨 云架构研究

沈光亮

(华为技术有限公司,北京 100010)

摘要: 从目前城市轨道交通信息化发展趋势出发,阐述在线网运营转型中面临的问题与挑战。结合《智慧城市轨道交通信息技术架构及网络安全规范》的要求,探讨城轨云架构作为基础平台在促进城市轨道交通信息化发展中的作用;研究云平台、网络安全、数据共享以及智能运维4个主要构成模块的功能与要求;重点探讨云平台作为城轨云架构的关键技术,其功能要求与技术选择将直接影响行业信息化的建设与发展;在具体工程项目中,应重点关注云平台技术的安全性、可靠性、稳定性以及可扩展能力,以统一服务“线网全业务、城轨多制式”为目标,构建一个开放的信息化基础平台。

关键词: 轨道交通;城轨云;云架构;云平台;信息化架构

中图分类号: U231

文献标志码: A

文章编号: 1672-6073(2020)05-0001-06

Urban Rail Cloud Architecture Based on Cloud Platform

SHEN Guangliang

(Huawei Technologies Co., Ltd., Beijing 100010)

Abstract: The problems and challenges in line operation transformation are described herein from the perspective of the current development trend of urban rail transit informatization. According to the *Smart city rail transit information technology architecture and network security specifications*, the design and development of the industry informatization involves several vital aspects: evaluation of urban rail cloud architecture as a basic platform in promoting the development of urban rail transit informatization; research on the functions and requirements of the cloud platform, network security, data sharing, and intelligent operation and maintenance O&M modules; and emphasis on the cloud platform as the key technology of the urban rail cloud

收稿日期: 2020-06-30 修回日期: 2020-08-03

作者简介: 沈光亮,男,本科,学士,从事城轨交通ICT解决方案规划设计,441707318@qq.com

architecture, its functional requirements, and technology choices. In real-world projects, the security, reliability, stability, and scalability of the cloud platform should be prioritized, and the building of an open information platform is suggested for all services of the urban rail network and the multiple modes of the urban rail.

Keywords: urban rail cloud; urban rail cloud architecture; urban rail cloud platform; urban rail informatics architecture

1 城轨信息化架构

城轨行业由线路运营向线网智慧运营转型过程中,面临信息技术资源重复建设、运维管理复杂,安全管控缺失等挑战。云计算、大数据等先进的信息通信技术(information and communication technology, ICT)的应用,正在推进行业网络化、智能化、智慧化发展,加速行业数字化转型。

2019年7月26日,中国城市轨道交通协会在北京发布了《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》)。《规范》明确提出采用城轨云架构来构建行业信息化平台,加速行业信息化发展与建设。

图1所示是城轨信息化1、3、5、3、1总体架构,也是整个城轨信息化建设的指导纲要^[1]。“1”是打造1个统一的城市轨道交通门户,实现信息服务的统一;“3”是规划3个城轨业务中心,包括生产指挥中心、企业管理中心以及乘客服务中心,提升运营、管理、服务效率;“5”是信息化建设涵盖城市轨道交通5大业务领域,包括运营生产、运营管理、企业管理、建设管理以及资源管理;“3”是按照业务性质和网络安全等级保护要求,构建安全生产、内部管理以及外部服务3张业务网络,承载城轨企业所有信息化业务;“1”是基于云计算技术,构建统一的城轨云平台。

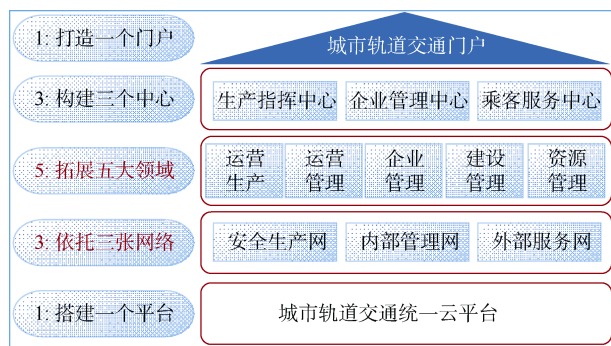


图1 城轨信息化总体架构

Fig. 1 Overall architecture of urban rail informatization

2 城轨云架构

城轨云作为支撑城轨信息化的平台架构,既要符合“13531”的总体设计原则,又要能很好地支撑信

息化业务的发展及各业务中心的建设。

当前,城轨行业进入一个高速发展时期,也加速了线路运营向线网智慧运营的转型。在新的运营模式下,对资源共享、运维管理以及业务安全防护都提出更高要求,而传统基于线路/专业系统的分散式建设,很难支撑城轨交通的网络化运营。由云平台、网络安全、数据共享以及智能运维等构成的城轨云架构,实现了信息技术资源的按需服务、数据的融合共享、运维的集中管理以及安全的统一管控,有效地解决了网络化运营面临的挑战,使其成为行业数字化转型中必不可少的基础平台架构。

2.1 云平台

2.1.1 物理部署

云平台基于云计算技术把各信息化业务分散部署的计算、存储等物理资源融合在一起,实现资源池化,统一为上层业务按需提供服务,提升整体资源利用率。云平台物理部署架构分为数据中心级云计算平台和站段云节点^[2]。

数据中心级云计算平台主要包含云管理平台、资源管理平台、虚拟化或容器等组件,支持智慧城轨服务保障和云服务编排。为确保业务的连续性,采用分布式云数据中心架构,按需为业务系统规划容灾级别,如综合监控系统(ISCS)、自动售检票系统(AFC)实现业务级容灾,在全自动驾驶模式下实现业务的双活容灾。考虑到线路持续新增扩容及机房空间的限制,云平台的规划应具备很好的扩展性,支持不同业务的主用/灾备中心部署在不同的地理位置。

站段云节点通过站段网络与数据中心云计算平台进行数据信息交换,站段云节点规划虚拟化云主机服务,分别为车站生产运营业务、企业信息管理类业务以及乘客信息服务类业务提供资源服务。

2.1.2 业务网络

云平台为安全生产网、内部管理网及外部服务网业务提供统一的IaaS(基础设施即服务)、PaaS(平台即服务)及SaaS(软件即服务)云服务。基于城轨信息化业务安全等保要求及云服务的灵活部署诉求,3张业务网分别规划独立的资源池,确保各资源池的安全性及IaaS、PaaS及SaaS云服务的按需部署。

安全生产网云资源池分为数据中心云资源池、车站云节点资源池。数据中心云资源池以专业系统规划 VDC, 专业系统内部按照线路规划 VPC; 车站云节点资源池规划统一 VDC, 按照不同专业系统规划 VPC。

内部管理网只在数据中心规划云资源池, 数据中心云资源池以业务领域规划 VDC, 各业务领域下具体应用规划 VPC; 车站办公终端通过车站接入网络、经骨干传输网络与数据中心服务连接。

外部服务网云资源池分为数据中心云资源池、车站云节点资源池。数据中心云资源池根据业务类型规划 VDC, 各应用系统规划 VPC; 车站云节点资源池规划统一 VDC, 各具体业务应用规划 VPC。

2.1.3 资源池规划原则

当前城轨信息化业务发展对云平台的 IaaS 服务需求最明确, 而计算、存储、网络以及安全资源池成为云平台建设的基础功能。资源池依据各信息化业务需求建设, 在《规范》明确规定业务需求的基础上, 重点解析资源池规划的原则。

1) 计算资源池: 计算资源池主要涉及云主机、裸金属两大类服务; 在具体工程中, 对业务应用采用云主机服务, 对业务数据库采用裸金属服务。

2) 存储资源池: 分布式存储、集中存储是当前两种主要的存储架构; 在具体工程中, 对业务数据库采用集中存储来构建资源池, 对业务应用或者桌面云应用可采用分布式存储来构建资源池。

3) 网络资源池: 网络资源池与 SDN 技术密切相关, 而 SDN 又分为软件 SDN、硬件 SDN; 一般来说, 软件 SDN 的兼容性更好, 而硬件 SDN 的性能更优。因此, 在具体工程中, 网络架构扩容、变更频繁的业务宜采用软件 SDN, 网络架构稳定且业务时延敏感的业务宜采用硬件 SDN。

4) 安全资源池: 云安全与物理网络安全是强相关的。在具体工程中, 应整体规划物理网络安全与云安全服务, 才能真正满足等保要求。

2.2 网络安全

网络与安全的设计是密不可分的。在城轨云架构下, 安全策略设计的总体原则是“系统自保、平台统保、边界防护、等保达标、安全确保”。其中, 三网间采用物理/逻辑隔离技术, 实现强管控; 网内各安全域则根据业务需要规划安全防护策略^[3]。

为更好地支撑安全策略设计, 依据“横向到边, 纵向到底”的网络架构总体设计原则, 规划安全生产、

内部管理、外部服务的 3 张业务网, 实现不同安全等级的信息化业务的隔离部署; 且 3 张业务网从线网中心、车站、车载纵向贯穿到底, 确保网内业务端到端的安全防护。

按照网络安全等保 2.0 的要求、《规范》的规定及城轨行业信息化业务需要, 安全生产网按照三级等保要求建设, 内部管理网按照二级等保要求建设, 外部服务网不作为等保硬性要求。

为实现统一运维, 在 3 张业务网之外, 规划单独的运维管理网, 主要承载运维管理相关的业务, 且与 3 张业务网采用独立的安全设备进行强管控。

2.3 数据共享

在城轨云架构下, 各信息化业务不仅实现计算、存储、网络、安全等资源的统一服务, 其数据共享也实现集中管控。数据共享平台为各业务提供标准的数据共享与数据接入接口, 并对数据共享的业务统一鉴权, 大大降低数据共享接口开发的复杂性, 大幅提升数据共享的效率与安全。

为协同网络安全设计, 数据共享平台按照安全生产网、内部管理网、外部服务网分域逻辑部署, 不同网间的大数据平台域的信息交换按照安全等级, 通过安全信息通道进行。

2.4 智能运维

城轨云的建设不仅是构建一个信息化平台, 更重要的是支撑信息化业务的安全、稳定、可靠的运行。由于城轨云尚处于建设运营初期, 绝大部分地铁的系统运维人员缺乏相应的运营、运维能力。因此, 针对城轨云较复杂的架构设计, 需要有一个智能化的综合运维平台, 简化运维管理, 降低能力要求。

智能运维平台实现了服务器、存储、网络、安全等硬件设备, 云平台、网络安全策略以及数据中心等的一体化管理; 通过“监(监控与告警)、管(配置管理)、控(自动化运维)、营(可视化)、服(流程管理)、智(智能化)”6 大核心功能, 实现“可视、智能、易用、开放”的数字化运维新体验, 为城轨行业提供一个高效率、高质量、运营结果可视化的统一运维平台。

3 云平台技术

云平台是城轨云架构的基石与底座, 而云计算又是云平台建设的关键核心技术, 应采用业界主流的开源云平台框架 OpenStack, 充分融入行业生态, 实现硬件、软件厂商无关性, 最大限度地保证客户既有的建设投资。各城市地铁在持续建设, 云平台要具备未

来几十条线路接入的扩展能力，业务资源的分配可根据应用负荷进行弹性伸缩^[4]。

云平台架构一般由基础设施硬件(服务器、存储、网络、安全等硬件设备)、虚拟化资源池、云服务以及云管理平台等部分组成。其中，基础设施硬件标准化程度最高，各云平台厂家都有对应的兼容性测试及清单，主流厂家的对接技术风险小；云管理平台模块一般由云平台厂家自定义,通过开放 API 接口实现对接。笔者主要对虚拟化、云服务进行研究分析。

3.1 虚拟化技术

3.1.1 全虚拟化(full virtualization)

全虚拟化也称为原始虚拟化技术，使用虚拟机协调 Guest 操作系统和原始硬件，操作系统是通过 Hypervisor 来分享底层硬件。全虚拟化主要是在客户操作系统和硬件之间捕捉和处理对虚拟化敏感的特权指令，使客户操作系统无需修改就能运行，不同的实现方式处理速度有差异，但均能满足用户的需求。全虚拟化的运行速度快于硬件模拟，但是性能方面不如裸机，因为 Hypervisor 需要占用一些资源。Guest OS 无需修改，速度和功能都非常不错，更重要的是使用非常简单。借助于硬件辅助虚拟化技术，可以解决 I/O 性能问题，是当前虚拟化技术的主流。

3.1.2 半虚拟化(para virtualization)

半虚拟化与全虚拟化有一些类似，它也是利用 Hypervisor 实现对底层硬件的共享访问，但是由于在 Hypervisor 上面运行的 Guest OS 已经集成与半虚拟化有关的代码，使得 Guest OS 能够非常好地配合 Hyperivovsr 来实现虚拟化。通过这种方法将无需重新编译或捕获特权指令，其性能非常接近物理机，最经典的产品就是早期的 Xen。这种模式和全虚拟化相比架构更精简，而且在整体速度上有一定的优势。因为需要对 Guest OS 进行修改，所以用户体验较差，不再是虚拟化技术发展的主流。

3.2 云服务技术

云服务是云平台提供给上层应用的各种服务能力，根据服务的内容及面向对象不同，一般分为 IaaS、PaaS、SaaS。其中，IaaS 提供计算、存储、网络、安全、容灾等基础的 IT 资源服务；PaaS 提供应用运行和开发环境及开发组件等平台性服务；SaaS 提供互联网 Web 应用、企业应用(ERP/CRM 等)等应用服务。当前各云平台厂家在 IaaS 能力上非常成熟，能提供的服务差异不大；而 PaaS 领域正处于快速发展阶段，也是

各厂家竞争的焦点；SaaS 服务的行业属性较强，目前在企业应用领域有较多应用。云服务内容如表 1 所示。

表 1 云服务内容
Tab. 1 Urban rail cloud service content

服务类型	服务内容	
IaaS 服务	计算服务	1) 裸金属服务 2) 弹性云主机服务
	储存服务	3) 云硬盘服务 4) 对象存储服务
	网络服务	5) 虚拟私有云服务 6) 安全组服务 7) 虚拟防火墙服务 8) 弹性负载均衡服务
	安全服务	9) 主机安全服务 10) 数据库审计服务 11) 云堡垒机服务 12) 安全态势感知服务 13) 漏洞扫描服务
	灾备服务	14) 云服务器备份服务 15) 云硬盘备份服务 16) 文件和数据库备份服务 17) 云服务器容灾服务 18) 云服务器高可用服务 19) 云硬盘高可用服务 20) 文件和数据库容灾服务
PaaS 服务	21) 数据库服务 22) 大数据计算服务 23) 大数据治理与开发服务 24) 视频智能分析服务 25) 应用与数据集成平台服务	
SaaS 服务	SaaS 服务主要是把通用的应用系统部署在相应的 IaaS、PaaS 上，以服务的形式为最终用户提供业务应用。不仅避免应用系统的重复投资建设，又让业务应用的上线更快捷	

1) 裸金属服务：为用户提供专属的物理服务器，提供卓越的计算性能，满足核心应用场景对高性能、稳定性、高安全性的需求。

2) 弹性云主机服务：由 CPU、内存、镜像、云硬盘组成的一种可随时获取、弹性可扩展的计算服务器，同时结合 VPC、安全组、数据多副本保存等能力，为业务打造一个高效、可靠、安全的计算环境，确保业务服务持久稳定运行。

3) 云硬盘服务：一种虚拟块存储服务，主要给云主机和裸金属提供块存储空间。用户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。

4) 对象存储服务：是一个基于对象的海量存储服务，为业务提供海量、安全、高可靠、低成本的数据存储能力。

5) 虚拟私有云服务: 用于构建隔离的、用户自主配置和管理的虚拟网络环境, 提升云资源的安全性, 简化业务的网络部署。

6) 安全组服务: 用来实现组内和组间的访问控制, 加强虚拟机的安全保护, 实现虚拟私有云内部的网络隔离。

7) 虚拟防火墙服务: 用于子网级别的安全防护, 是一个或多个子网的访问控制策略, 根据与子网关联的入站/出站规则, 判断数据包是否允许流入/流出关联子网。

8) 弹性负载均衡服务: 将访问流量自动分发到多台弹性云服务器, 扩展应用系统对外的服务能力, 实现更高水平的应用程序容错性能。

9) 主机安全服务: 提供主机入侵防御等安全功能, 保障弹性云主机的安全性。

10) 数据库审计服务: 为数据库提供用户行为发现审计、多维度分析、实时告警和报表等功能, 保障云上数据库的安全, 满足业务合规要求。

11) 云堡垒机服务: 通过网络内部署云堡垒机, 使其成为运维的唯一入口, 连接 windows 服务器、linux 服务器、数据库等资产时都必须经过云堡垒机的统一身份管理, 并基于 IP 地址、账号、命令进行控制, 防止越权操作, 而且整个操作过程都可以实现全程的审计记录。

12) 安全态势感知服务: 通过收集其他各服务授权的海量数据, 对用户的安全态势进行多维度集中、简约化呈现, 方便用户从大量的信息中发现有用的数据。同时, 结合大数据挖掘和分析技术, 提供全覆盖的从对手分析到全局分析的能力, 帮助用户准确理解过去发生的每一件安全事件, 以及预测将来有可能发生的安全事件。

13) 漏洞扫描服务: 以 Web、数据库、基线核查、操作系统、软件安全检测为核心, 弱口令、端口与服务探测为辅助的综合漏洞探测系统。

14) 云服务器备份服务: 可为云主机和裸金属创建整机备份, 利用备份数据恢复云服务器业务数据, 最大限度保障业务数据的安全性和正确性, 确保业务安全。

15) 云硬盘备份服务: 为云硬盘创建备份, 利用备份数据恢复云硬盘, 最大限度保障用户数据的安全性和正确性, 确保业务安全。

16) 文件和数据库备份服务: 融合数据备份与恢复、数据异地容灾、数据高可用等功能, 支持业务的共享使用与逻辑隔离, 以及本地数据中心业务和云端

数据业务的协同保护。

17) 云服务器容灾服务: 为云服务器提供跨 Region 异地容灾保护, 当生产中心发生灾难时, 可在异地容备中心恢复受保护的云服务器。

18) 云服务器高可用服务: 为云服务器提供同城数据中心间的高可用保护。当生产中心发生灾难时, 被保护的云服务器能够自动或手动切换到灾备中心。

19) 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。

20) 文件和数据库容灾服务: 将容灾资源云化、服务化, 为业务提供快速、按需的企业级文件和数据库容灾服务, 实现业务云下本地数据中心业务和云端虚拟数据中心业务的统一保护能力, 保证业务数据的安全性和连续性。

21) 数据库服务: 基于云计算平台的即开即用、稳定可靠、弹性伸缩、便捷管理的在线关系型数据库服务(具体支持的数据库类型, 各厂家有差异)。

22) 大数据计算服务: 为业务提供高性能、低成本、灵活易用的全栈大数据平台, 运行 Hadoop、Spark、HBase、Kafka、Storm 等大数据组件, 并具备在后续根据业务需要进行定制开发的能力。

23) 大数据治理与开发服务: 数据全生命周期管理、智能数据管理能力的一站式治理运营, 支持行业知识库智能化建设, 支持大数据存储、大数据计算分析引擎等数据底座, 帮助企业快速构建从数据接入到数据分析的端到端智能数据系统, 消除数据孤岛, 统一数据标准。

24) 视频智能分析服务: 依靠 AI 技术对视频进行智能分析, 提供视频预处理、视频审核、视频内容分析、视频编辑、视频搜索、视频指纹等功能, 包含对视频中目标的检测、跟踪、属性识别、行为识别、内容审核、摘要、标签等能力, 在多种场景下为用户提供快捷高效的视频分析能力。

25) 应用与数据集成平台服务: 聚焦应用和数据连接, 适配多种企业常见的使用场景。提供轻量化消息、数据、API、设备等集成能力, 简化企业上云, 支持云上云下、跨区域集成, 帮助企业实现数字化转型。

4 城轨云架构的关键技术要求

城轨云架构不仅要覆盖城轨所有信息化业务, 同时也要服务于城轨所有制式。因此, 城轨云架构的安全性、可靠性、稳定性、可扩展能力非常重要。

4.1 安全性

城轨云架构下,资源使用方式和管理方式的变化带来了新的安全风险和威胁。对管理员而言主要存在的风险和威胁包括虚拟管理层成为新的高危区域、恶意用户难以被追踪和隔离、云计算的开放性使云计算系统更容易受到外部攻击;而对最终用户而言,使用云计算服务带来的主要风险和威胁包括数据存放在云端无法控制的风险、资源多租户共享带来的数据泄露与攻击风险、网络接口开放性的安全风险。

云平台架构针对所面临的安全威胁与挑战,应能提供相应解决方案,并按照防护对象的不同,分成基础设施安全和租户安全。基础设施安全又细分为边界安全、云操作系统安全、云服务安全和安全管理;而租户安全分为网络安全、主机安全、应用安全、数据安全、安全管理。整个方案从预测、防护、检测和响应4个维度展开,实现全方位的安全防护。

1) 防护:是基于策略或者特征,尽量减少整个系统的被攻击面,防止攻击事件发生。例如加固/保护应用、诱骗攻击者等都是可以利用的方式。

2) 检测:用于发现逃过防御网络的攻击,需要持续监控,通过网络中的日志、安全事件或者通过流量里面的一些行为,构建检测能力;发现被攻击,才能采取行动去防止事件升级,降低损失。

3) 响应:响应高效及时,马上更新策略、给系统打上补丁、加入新的特征。同时,通过审计数据或相应的记录进行溯源,查出、记录搞破坏者,支撑调查取证。

4) 预测:通过防御、检测、响应结果不断优化基线系统,主动进行风险评估,从外部发现黑客正在进行的一些破坏,整理出信息、情报,逐渐精准预测未知的、新型的攻击。

4.2 可靠性

城轨云架构承载的是多条线路多个专业系统,架构的可靠性非常关键。云平台从多个层面来保障架构的可靠性。

1) 业务层面:具体保障能力有架构的物理容灾、计算/存储资源 HA、计算和存储、快照和恢复、弹性 IP 等。

2) 平台层面:具体保障能力有节点 HA、故障管理、负载均衡、流控、数据一致性、资源动态调度与热点消除、存储多路径访问、分布式事务机制、网络平面隔离等。

3) 硬件层面:具体保障能力有服务器电源、风扇冗余备份、内存软失效、内存隔离、网络多平面,存

储故障预警、热插拔、亚健康检测、故障隔离、故障自我修复等。

4) 管理层面:具体保障能力有告警、日志管理、配置管理、升级不中断业务管理,以及在线无损扩容、分布式集群等。

4.3 稳定性

随着云计算的发展,云服务能力将越来越丰富,而业务应用要持续获得云平台新的服务能力,必然会涉及版本的升级迭代。云平台升级时要保证既有城轨云架构下的硬件基础设施及业务软件的兼容性,确保升级过程中业务稳定运行。在产品规划层面,要求版本能持续迭代及平滑升级;在集成验证层面,要求提供较大规模的测试平台,模拟现网环境,充分测试验证,确保版本升级后业务稳定运行。

4.4 可扩展能力

城轨云架构初期可能只服务一条或者几条线路,后续将不断扩展,有可能达到十几条线甚至几十条线路的规模。在城轨云的持续建设过程中,一定会涉及多个厂商的产品,云平台的兼容性也是城轨云架构考量的关键要素。一方面云平台需要支撑 50 条线路服务能力,并具备 100 条线路扩展能力;另一方面云平台需要兼容主流厂家主流的硬件设备型号及其虚拟化平台。

5 结语

由城轨行业信息化的发展,引申出城轨云建设的必要性,重点研究了城轨云架构的构成,尤其是针对作为底座的云平台进行详细分析。城轨云的建设目标是服务于城市所有地铁线路及轨道集团的信息化业务,城轨云架构的安全、稳定、可靠、可扩展能力非常重要;作为支撑城轨云建设的关键技术——云计算技术的选择,也成为城轨云架构可持续发展的关键。

参考文献

- [1] 中国城市轨道交通协会. 智慧城市轨道交通 信息技术架构和信息安全规范 第1部分总体需求[R]. 北京, 2019.
- [2] 中国城市轨道交通协会. 智慧城市轨道交通 信息技术架构和信息安全规范 第2部分技术架构[R]. 北京, 2019.
- [3] 中国城市轨道交通协会. 智慧城市轨道交通 信息技术架构和信息安全规范 第3部分网络安全[R]. 北京, 2019.
- [4] 中国城市轨道交通协会. 城轨交通云平台构建及部署方案研究[R]. 北京, 2018.

(编辑:王艳菊)