ICS 45.020
CCS L 70

团 体 标 准

T/CCTAS XX—2024

粤港澳大湾区城际铁路线网云平台总体技术要求

General technical requirements for cloud platform of intercity railway in the Guangdong-Hong Kong-Macao Greater Bay Area

（征求意见稿）

2024 年 5 月 10 日

2024 - XX - XX 发布　　2024 - XX - XX 实施

中 国 交 通 运 输 协 会　　发 布

目　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由广东省交通运输厅提出。

本文件由中国交通运输协会标准化技术委员会归口。

本文件起草单位：广州地铁集团有限公司、深圳市地铁集团有限公司、广州地铁设计研究院股份有限公司、广东珠三角城际轨道交通有限公司、中国铁路设计集团有限公司、广州铁路投资建设集团有限公司、广东城际铁路运营有限公司、广州穗腾数字科技有限公司。

本文件主要起草人：

1 范围

本文件规定了城际铁路线网云平台的总体要求、云平台构成、功能要求、性能要求、网络安全要求、接口要求。

本文件适用于城际铁路线网云平台（以下简称云平台）的设计、建设及运营。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB 50157-2013 地铁设计规范

GB 50174-2017 数据中心设计规范

GB 51151-2016 城市轨道交通公共安全防范系统工程技术规范

GB/T 51399-2019 云计算基础设施工程技术标准

GB/T 20988-2007 信息安全技术信息系统灾难恢复规范

GB/T 22239《信息安全技术 网络安全等级保护基本要求》

TB 10623-2014 城际铁路设计规范

T/CAMET 11002—2020 城市轨道交通云平台构建技术规范

T/CAMET 11003—2020 城市轨道交通大数据平台技术规范

T/CAMET 11004—2020 城市轨道交通云平台网络架构技术规范

T/CAMET 11005—2020 城市轨道交通云平台网络安全技术规范

T/CAMET 11006—2020 城市轨道交通线网运营指挥中心系统技术规范

T/CAMET 11001.3—2019 智慧城市轨道交通 信息技术架构及网络安全规范 第 3 部分:网络安全

T/CAMET 11007—2022 城市轨道交通信息化工程设计规范

3 术语和定义

下列术语和定义适用于本标准。

3.1 云计算 cloud computing

一种通过网络将可伸缩、弹性的共享物理和虚拟资源池以按需自服务的方式供应和管理的模式。

注：资源包括服务器、操作系统、网络、软件、应用和存储设备等。

[来源：GB/T 31167-2014，3.1]

3.2 云平台 cloud platform

为用户提供云计算及云服务的各类软硬件系统、组件的集合，包括但不限于基础设施即服务、平台即服务、软件即服务等。

3.3 云节点 cloud node

云平台中独立于数据中心、分布式部署的、为用户提供少量云计算资源的节点。

3.4 数据中心 data center

为集中放置的电子信息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。

[来源：GB 50174-2017，2.1.1]

3.5 主用中心 primary center

主用系统所在的数据中心。

3.6 灾备中心 backup center for disaster recovery

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。

3.7 虚拟专有云 virtual private cloud

为虚拟数据中心虚拟出逻辑隔离的虚拟网络环境，包括但不限于虚拟子网、虚拟防火墙、虚拟路由器等。

3.8 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撑的平台。

3.9 安防集成平台 integrated security platform

通过统一的通信平台和管理软件对技术防范系统进行自动化管理与监控的分层分布式计算机集成系统。

[来源：GB 51151-2016，2.0.3]

3.10 资源池 resource pool

一组物理资源或虚拟资源的集合，可从池中获取资源，也可将资源回收到池中。资源包括物理机、虚拟机、物理网络设备、虚拟网络设备和 IP 地址等。

[来源：GB 51399-2019，2.1.3]

3.11 **虚拟机 virtual machine**

一种虚拟的数据处理系统，是在某个特定用户的独占使用下，但其功能是通过共享真实数据处理系统的各种资源得以实现的。

[来源：GB 51399-2019，2.1.4]

3.12 **容灾系统 backup system for disaster recovery**

用于灾难恢复目的，对数据、数据处理系统、网络系统、应用系统等进行备份的系统。

3.13 **云桌面 cloud desktop**

利用云计算技术集中部署客户端应用所需的操作系统和应用软件，通过桌面连接协议将完整的虚拟机桌面交付给用户终端使用。

3.14 **云管理平台 cloud management platform**

云计算环境的重要组成部分，对企业云平台各类同构、异构的物理资源、虚拟化资源等进行统一运维管理和运营管理的应用系统，对外提供云计算环境中各类计算、存储和网络资源等的交付服务。

3.15 **中台 middle platform**

一种灵活应对变化的架构，快速实现前端提的需求，为共享的开发资源所提供的业务能力、数据能力和计算能力的集合。

3.16 **容器 Container**

一种操作系统虚拟化形式。可以运行从小型微服务或软件进程到大型应用程序的所有内容。

4 缩略语

下列缩略语适用于本文件。

4.1 **IaaS：基础设施即服务（Infrastructure as a Service）**

4.2 **CPU：中央微处理器（Central Processing Unit）**

4.3 **QoS：服务质量（Quality Of Services）**

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

4.5 **SAN：存储区域网络（Storage Area Network）**

4.6 **API：应用程序编程接口（Application Programming Interface）**

4.7 **SDK：软件开发工具包（Software Development Kit）**

4.8 **VPC: 虚拟私有云（Virtual Private Cloud）**

4.9 **MTBF：平均故障间隔时间（Mean Time Between Failures）**

4.10 **MTTR：平均修复时间（Mean Time To Repair）**

4.11 **vCPU：虚拟处理器（Virtual Central Processing Unit）**

4.12 **FC：光纤通道（Fibre Channel）**

4.13 **FC SAN：光纤通道存储区域网络（Fibre Channel Storage Area Network）**

4.14 **IP SAN：IP 通道存储区域网络（IP storage Area Network）**

4.15 **iSCSI：internet 小型计算机系统接口（internet Small Computer System Interface）**

4.16 **RDMA:远程直接数据存取(Remote Direct Memory Access)**

4.17 **GE:千兆以太网(Gigabit Ethernet)**

4.18 **TVM：自动售票机（Ticket Vending Machine）**

4.19 **BOM：人工售票机（Booking Office Machine）**

4.20 **AGM：人工检票机（Automatic Gate Machine）**

4.21 **WIFI：无线保真（Wireless Fidelity）**

4.22 **TCP：传输控制协议（Transmission Control Protocol）**

4.23 **UDP：用户数据报协议（User Datagram Protocol）**

5 总体要求

5.1 云平台的设计和建设应与城际铁路线网规划及运营管理模式相适应，遵循统一规划、统一标准、资源共享的原则，符合安全、可靠、先进、兼容、可扩展的要求。

5.2 云平台应采用高可靠的设备，保证能全天候不间断地运行。

5.3 云平台应采用标准化、开放的接口形式及协议，实现业务系统间的互联互通、统一管理。

5.4 云平台应满足《信息安全技术 网络安全等级保护基本要求》GB/T 22239 第三级安全要求。

5.5 云平台应实现资源灵活分配、应用灵活部署、云边端协同管理、场景化业务动态调整功能。

5.6 云平台应构建统一的数字底座，各类应用通过在统一的数字底座上组件化设计和部署实现专业数据融合和经验共享。

5.7 云平台应支持多种虚拟化技术，应能兼容主流厂商的多种异构设备，应根据业务系统对云平台需求，选择通用的、绿色节能的服务器、存储和网络设备。

5.8 云平台应具有扩展性和开放性，软硬件可根据业务需求无损升级和扩展。

5.9 云平台应采用分层模块化技术，软件组件能够解耦，并开放接口，保证应用系统能够平滑迁移。

5.10 云平台应根据城际铁路线网业务管理模式，有效整合城际铁路线网各类业务应用的需求，建设开放部署环境及业务应用融合的云平台。

5.11 云平台应能为各业务应用提供计算、存储、网络等基础资源，并预留其他应用及功能组件开发接入的扩展能力，实现基础架构资源统一管理及动态分配，满足业务应用灵活应用开发的需求。

5.12 云平台应支持为不同业务提供不同深度、不同范围、不同组合形式服务的条件。

5.13 云平台需满足业界通用虚拟化、弹性计算、高等级安全、跨地理位置分布、大规模性、一致性等要求，并针对满足城际铁路业务系统对云平台架构的要求。

5.14 云平台技术架构不应存在单点故障，基础设备应具备高可靠性，重要组件应负载分担，关键组件应热备份，并应具备故障自动切换功能，不得影响系统正常运行。

5.15 云平台应在控制中心集中部署资源池，并考虑容灾部署，应设置统一云管理平台，为城际铁路线网的所有应用提供云服务。

5.16 云平台容灾部署应根据运营管理需要，确定相关业务应用系统的灾难恢复能力等级及容灾需求。

5.17 根据城际铁路智能运行平台、业务应用系统不同网域间信息交互的需求，综合业务云平台应采用安全隔离措施实现安全生产网、内部管理网、外部服务网之间的网域间安全互通。

6 云平台构成

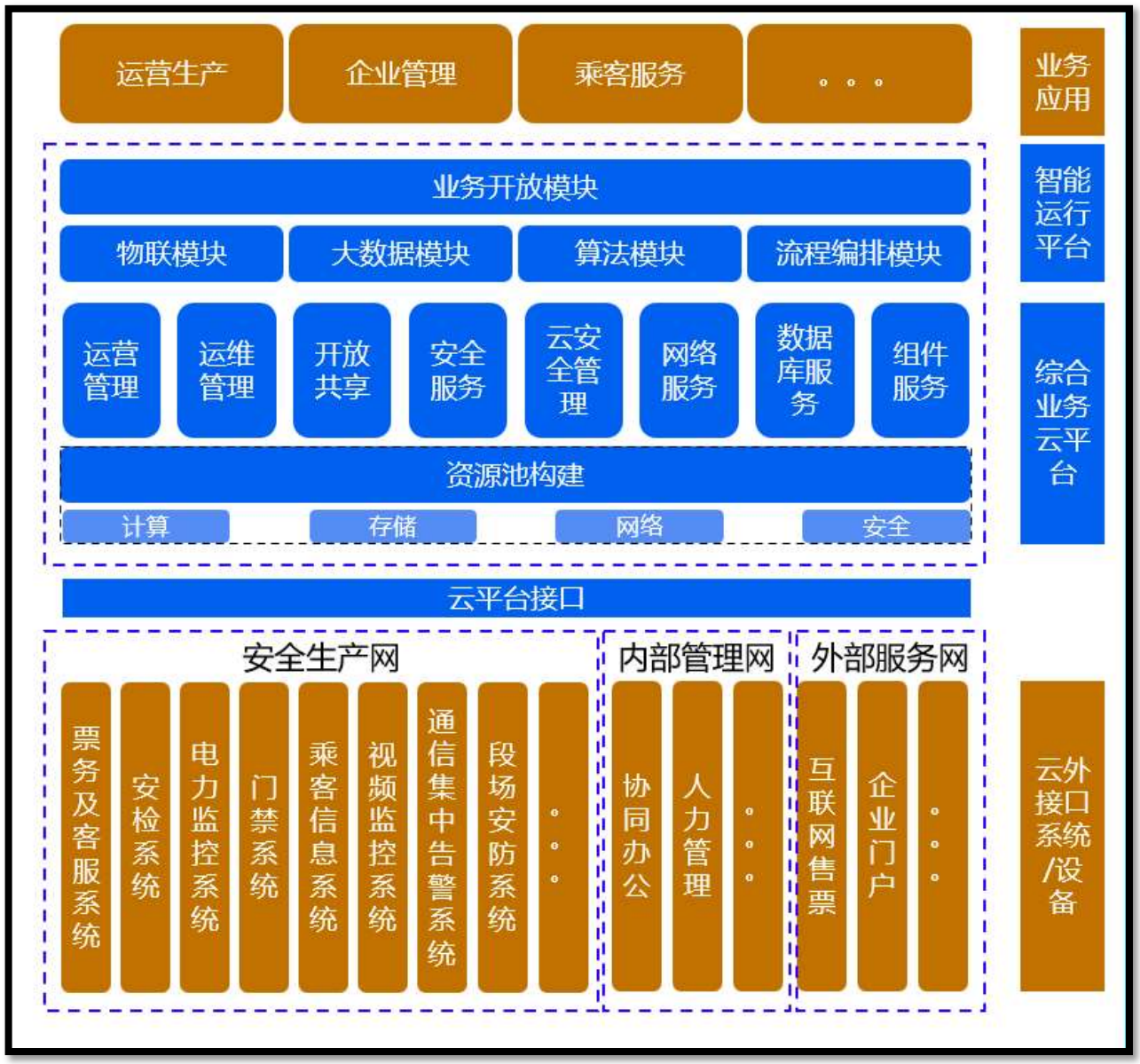

图 1 云平台技术架构图

6.1 云平台由综合业务云平台、智能运行平台及云平台接口构成。

6.2 综合业务云平台应为用户提供计算、存储、网络、安全等 IT 基础设施资源及封装后的多种 IaaS 服务；综合业务云平台宜在车站及段场设置边缘计算节点，满足业务应用边缘计算、高实时性的需求，同时也可作为降级后备使用。

6.3 智能运行平台宜包含物联模块、大数据模块、算法模块、流程编排模块、业务开放模块等服务。

6.4 云平台应为城际铁路线网业务应用提供开发部署环境以便各业务应用在该环境上实现运营生产、运营管理、企业管理、资源管理、建设管理及乘客服务等各项功能。

6.5 云平台接口宜包括安全生产网接口、内部管理网接口、外部服务网接口。

6.6 安全生产网宜包括票务及客服系统、综合监控/轨道交通综合管理指挥应用、安检系统、电力监控系统、门禁系统、乘客信息系统、视频监视系统、车辆智能运维系统、轨道监测系统、信号运维保障系统、通信智能监测管理平台/通信集中告警系统、自动扶梯部件预警系统、段场安防系统等安全运营生产类业务系统，可结合城际铁路业务系统运营及维护的需要进行调整。

6.7 内部管理网宜包括协同办公领域、财务管理领域、人力管理领域、项目管理领域、建设管理领域、运营管理领域等业务系统。

6.8 外部服务网宜包括乘客服务管理系统、视频监视系统、互联网售票系统、企业门户网站、互联网信息以及政府管理机构外部系统等。

7 功能要求

7.1 综合业务云平台

7.1.1 资源池构建

7.1.1.1 综合业务云平台可根据各业务系统对计算、存储、网络、安全资源的需求，设置相应的资源池。

7.1.1.2 各类业务应用系统宜设置共用存储资源池，根据应用系统存储需求可采用 SAN 集中式存储系统或基于服务器的分布式存储系统。

7.1.1.3 综合业务云平台可根据各业务系统的不同需求，对资源进行灵活分配，需同步具备资源规格可动态调整、资源利用率高、安全性强等特点。

7.1.1.4 综合业务云平台应根据各业务系统的特点，对于存储进行不同的选型，对存储对象进行分级管理。

7.1.1.5 综合业务云平台应为各个业务系统的应用部署提供自助式的网络交互服务，且网络资源池应能确保各业务系统网络之间的安全隔离与互通。

7.1.1.6 综合业务云平台应具备统一资源管理的功能，云平台的升级和资源配置，不应影响业务系统的正常运行。

7.1.1.7 综合业务云平台应兼容 X86 服务器、ARM 服务器等，并能够运行的主流操作系统（包括国产化操作系统）。

7.1.2 运营管理

7.1.2.1 综合业务云平台应支持“分权分域”管理，即不同管理员分配不同管理范围和业务访问权限，方便不同部门、不同组织的管理员的业务分工。

7.1.2.2 综合业务云平台应内置多种通用服务组件，并支持动态扩展。通用服务组件应包括但不限于权限控制、工作流引擎、数据服务、服务目录、服务门户、可视化报表、资源计量、API 网关、搜索引擎等。

7.1.3 运维管理

7.1.3.1 综合业务云平台应提供涉及计算、网络与存储所需的各类技术环境的管理，并具备多中心统一管理的能力，同时应为各类应用提供包括但不限于系统测试、应用发布、应用运行、系统维护所需的技术环境，应提供包括但不限于用户管理、资源管理、运行维护管理等功能。

7.1.3.2 综合业务云平台应具备基于角色的用户权限控制功能，包括但不限于用户管理、角色管理、角色授权、登陆认证等功能，同时对于角色和操作权限管理，不同角色可对应不同的操作权限，不同的操作用户可对应于不同的角色。

7.1.3.3 综合业务云平台应具备运维管理功能，可将不同维度的云资源（包含但不限于计算、存储、网络）的性能、告警信息综合分析，以直观的界面呈现业务的实时状态，包括但不限于告警管理、资源管理、敏捷报表、基础设施监控、资源池监控等功能模块，可支撑日常运维、系统变更、运营分析等运维业务场景，并可实现多个数据中心的集中运维管理。

7.1.3.4 综合业务云平台应具备监控管理功能，包括但不限于阈值管理、状态管理、性能管理、容量管理、机房环境管理等，其中监控对象应包括但不限于集群资源、物理资源、计算资源、存储资源、网络资源等，并可整合性能、告警以及其强关联资源数据，协助管理员进行故障排查。

7.1.3.5 综合业务云平台应具备告警管理功能，包括但不限于告警集中查询、告警全生命周期管理、告警分析、告警收敛等，在集群资源、物理资源、计算资源、存储资源、网络资源出现故障时，可根据预设的告警规则及时发出告警信息，告警方式包括但不限于邮件、短信或其它通信方式。

7.1.3.6 综合业务云平台应具备日志管理功能，记录管理员的操作日志与平台的运行日志，以便于后续安全审计、故障点定位等。

7.1.3.7 综合业务云平台应具备内存分配管理功能，可通过优化或采用容器技术减少虚拟化软件的性能损耗。

7.1.3.8 综合业务云平台应具备虚拟机/容器的 CPU QoS 控制管理功能，能控制虚拟机/容器获得的计算资源能力，控制虚拟机/容器获得的最大计算能力以及修改虚拟机的配置参数。

7.1.3.9 综合业务云平台应具备对所有物理资源、虚拟化资源进行统一管理功能，实现资源快速发放，缩短业务上线时间等。

7.1.3.10 综合业务云平台应具备对各种物理资源、虚拟化资源数据统一建模功能，将云平台资源以业务系统可见的资源池形式提供给业务系统应用。

7.1.3.11 综合业务云平台应具备对资源分集群管理功能，包括但不限于集群的创建、删除、扩容、缩容等，并应对集群进行性能监控。

7.1.3.12 综合业务云平台应具备虚拟机/容器全生命周期管理功能。

7.1.3.13 综合业务云平台应具备存储资源的管理功能，包括但不限于文件存储、块存储、对象存储等存储资源，并应支持向存储资源池中增加、删除数据存储，对已存在的数据存储可以扩容。

7.1.3.14 综合业务云平台应具备负载均衡功能，能够根据计算节点 CPU、存储等资源的使用情况，进行资源均衡分配。

7.1.3.15 综合业务云平台应具备弹性伸缩功能，通过设置不同的调度策略，实现智能资源调度，保证资源的合理分配，满足虚拟机/容器应用对资源弹性伸缩的需求。

7.1.3.16 综合业务云平台应具备资源切换管理功能，可把虚拟机/容器从故障的云平台节点上迁移至正常的云平台节点。

7.1.3.17 综合业务云平台应具备多种调度方案管理功能，包括但不限于在指定的节点上运行、在划定物理域内调度，全局调度等。

7.1.3.18 综合业务云平台应具备容器间亲和关系管理功能，包括但不限于多容器间可以绑定关联部署在同一个物理机、以分离关系部署在不同的物理机等。

7.1.3.19 综合业务云平台应提供统一的图形界面管理软件，可以在同一页面完成所有虚拟机、物理机以及容器等资源的日常管理工作。

7.1.4 **开放共享**

7.1.4.1 综合业务云平台应具备集成开发的能力，能对外提供 SDK 包，支持多种开发语言，方便第三方系统的快速集成开发，实现对综合业务云平台的灵活操作与管理。

7.1.4.2 综合业务云平台应具备开放 API 接口的能力，第三方系统可通过 API 接口获取到各种资源信息，包括但不限于集群信息、服务器资源、虚拟机信息、容器信息、网络信息、监控告警信息等。同时，第三方系统还可以通过 API 接口对资源进行操作维护，包括但不限于支持对虚拟机的生命周期管理，包括启动、停止、重启等操作。

7.1.5 网络服务

7.1.5.1 综合业务云平台应具备云内软件定义网络能力，应为各个业务系统的应用部署提供对应网络交互服务，网络资源池应能确保各业务系统网络之间的安全隔离与互通，且应具备 VPC 专网管理等能力。

7.1.5.2 综合业务云平台应具备网络资源的管理功能并集成软件定义网络，可通过 SDN 对基础网络设备进行操作和编排，实现网络资源的自动化操作与交付。

7.1.6 数据库服务

7.1.6.1 数据库服务应采用裸金属服务器的计算节点通过网络联接并协同工作，对外提供统一的数据管理与服务功能。

7.1.7 组件服务

7.1.7.1 综合业务云平台应内置多种通用服务组件，并支持动态扩展。服务组件应包括权限控制、工作流引擎、消息中间件等。

7.2 智能运行平台

7.2.1 智能运行平台应提供统一的数字底座、持续迭代的开发部署环境，并与各类业务应用共建行业组件库。

7.2.2 智能运行平台应充分利用所管辖各类业务的海量数据资源，构建融合共享、安全可靠的数据平台，深度挖掘数据的资源价值，形成持续的数据整合与应用能力。

7.2.3 智能运行平台应融合智能感知、大数据、人工智能等技术应用。

7.2.4 智能运行平台应采用中台技术、大数据技术进行构建，实现各专业数据融合和规则共享，并为各专业的数据分析及辅助决策提供数据支撑服务。

7.2.5 智能运行平台各模块间应采用解耦方式设计，适应应用需求支持模块调整及扩展的需求。

7.2.6 物联模块应具有物联化标准接入、协议转换、边缘数据处理及标准物联开放能力。

7.2.7 大数据模块应具备统一的数据接入标准，应具备基于所管辖各类业务的海量数据的数据采集、过滤、清洗、检索、建模、挖掘、分析、可视化与数据服务等能力，并与各专业以组件化形式共建数据服务组件。

7.2.8 算法模块应具备轨道交通各专业算法向导式构建和统一托管能力，需提供从模型构建、算法迭代到算法部署、算法服务的全生命周期支撑。

7.2.9 流程编排模块应具备基于交互式流程编排与计算的业务场景构建能力，提供贴合轨道交通业务人员操作习惯的拖拉拽式可视化逻辑画布，实现轨道交通各式业务流程的灵活编排。

7.2.10 业务开放模块应具备基于高内聚低耦合、数据完整性、业务可运营性、渐进性等原则形成组件化的共享服务，并应具备汇聚协同的各类业务组件能力。

7.2.11 智能运行平台应支持结构化数据、半结构化数据和非结构化数据等多源异构数据的接入与融合。异构数据源采集应包括实时信息、实时文件、多媒体数据、数据库实时同步、数据库批量采集方式。

7.2.12 智能运行平台数据治理应符合以下规定：

a）数据预处理：数据预处理应包括数据清洗与数据转换两部分功能，数据清洗负责过滤不符合要求的数据，数据转换负责将数据按规则进行规整；

b）数据批处理：数据批处理应用于时效性要求不高、同时数据处理规模较大的场景；

c）流数据处理：流数据处理适用于数据处理结果需要高效低延迟的场景，应支持流式数据的处理与计算。

7.2.13 智能运行平台数据服务应提供标准的、开放的服务 API 接口或协议，建立完善的数据服务申请和审核机制，并在服务过程中实时进行服务监控与分析，对平台中所有的服务进行统一管理、统一监控，保障内外部数据服务的安全。

7.2.14 安全生产网大数据平台应符合网络安全等级保护三级要求，内部管理网大数据平台宜符合网络安全等级保护二级要求。

7.2.15 大数据平台应采用数据隔离、系统安全、数据安全、权限安全、数据加密、平台审计、数据仓库安全等安全策略，具体技术要求应符合 T/CAMET 11005—2020 中 7.5 的规定。

7.2.16 业务开放模块 API 接口、中间件及数据安全应符合 T/CAMET 11001.3—2019 中 8.4 的要求。

8 性能要求

8.1 通用性能

8.1.1 MTBF≥10000 小时。

8.1.2 MTTR≤0.5 小时。

8.1.3 任何冗余的网络设备发生单点故障，不应影响系统的正常工作。

8.1.4 软件采用模块化设计，单个模块故障不应引起数据的丢失和系统的瘫痪。

8.1.5 可用性不小于 99.98%。

8.1.6 常用操作页面响应时间<=1s。

8.1.7 常用统计页面相应时间<=2s。

8.1.8 单台云主机创建耗时（不包含云主机启动时间）<=25s。

8.1.9 单台云主机快照恢复耗时<=1 分钟。

8.1.10 云硬盘单盘创建耗时<=10s。

8.1.11 云硬盘单盘快照创建或恢复耗时<=1 分钟。

8.1.12 云平台调度 API 接口响应时间<=2s。

8.2 计算资源池性能

8.2.1 单个虚拟化计算资源池集群可支持不少于 128 台物理服务器。

8.2.2 计算虚拟化软件占用物理服务器 CPU 的资源占用率不宜高于 5%。

8.2.3 单台虚拟机规格可支持 64 个 vCPU、1TB 内存、12 块网卡、12 块磁盘。

8.3 存储资源池性能

8.3.1 集中式 SAN 存储系统性能应符合下列规定：

a) 系统架构应采用高可用架构，安全生产网存储系统存储控制器配置不应少于 2 控，可扩展为 8 控；内部管理网、外部服务网存储系统存储控制器配置不应少于 2 控，可扩展为 4 控；

b) 安全生产网存储系统存储缓存配置不应少于 1TB；内部管理网、外部服务网存储系统存储缓存配置不应少于 256GB；

c) FC SAN 存储网络应支持不小于 8Gbit/s FC，IP SAN 存储网络应支持不小于 10Gbit/s iSCSI 以保障集中式 SAN 存储性能；

d) 安全生产网存储系统存储远程异步复制方式异步传输时间间隔宜小于 5 分钟，内部管理网、外部服务网存储系统存储异步远程复制方式异步传输时间间隔宜小于 10 分钟。

8.3.2 分布式存储系统性能应符合下列规定：

a) 单个存储集群最大可支持 4096 个存储节点；

b) 存储系统多节点并行恢复 1TB 数据应小于 30 分钟；

c) 存储系统的节点扩容时间不应大于 30 分钟/批，每批次节点数不应少于 100 个；

d) 存储网络应支持不小于 10G 的以太网，支持 RDMA 访问协议，保障分布式存储性能。

8.3.3 视频云存储系统的性能应符合下列规定：

a) 存储节点采用控制器架构时，每台存储设备应配置不少于 2 个控制器，每个控制器应有独立的中央处理器；控制器之间采用并行运行、负荷分担工作方式；

b) 存储节点采用服务器架构时，单台存储设备宜配置不少于 2CPU；

c) 单个存储集群最大可支持 288 个存储节点，集群范围内能够实现动态负载均衡；

d）采用 4Mb/s 码流时，单台存储节点并发存储能力应≥300 路；采用 2Mbit/s 码流时， 单台存储节点并发存储能力不应小于 600 路；

e）单台存储节点网络接口数量不小于 4×GE 或不小于 2×10GE；

f）单台存储节点缓存不小于 32GB；

g）支持写缓存镜像，写缓存断电后对数据存储的保护时间不小于 100 小时；

h）支持集群内跨存储节点的冗余保护功能，应至少支持任意两块硬盘或者任意一个节点故障时数据不丢失，业务不中断；单集群最大可支持 4 个存储节点故障时数据不丢失，业务不中断；

i）为了确保数据可靠性，全盘数据重构速率达到 1TB/小时。

8.4 数据备份系统性能

8.4.1 单台备份介质服务器最大支持备份重删后的数据量不小于 100TB。

8.4.2 备份软件的性能要求应符合下列规定：

a）备份软件重删块最大可支持 512KB；

b）单个服务器支持备份的虚拟机以挂载的方式分钟级恢复虚拟机；

c）本地备份速度宜不小于 500Mbit/s，恢复速度宜不小于 300Mbit/s；

d）异地备份速度宜不小于 300Mbit/s，恢复速度宜不小于 100Mbit/s。

8.4.3 采用集中式 SAN 存储或 NAS 存储系统作为备份存储设备的性能要求应符合下列规定：

a）系统架构应采用多控制器冗余架构，控制器配置不应少于 2 控；

b）每个存储控制器的存储缓存（Cache）配置不应小于 256GB；

c）FC SAN 存储网络应支持不小于 8Gbit/s FC，IP SAN 存储网络应支持不小于 10Gbit/s iSCSI 以保障集中式 SAN 存储性能。

8.5 虚拟机容灾性能

8.5.1 相关业务应用系统的灾难恢复性能应符合《信息安全技术信息系统灾难恢复规范》（GB/T 20988 中相应灾难恢复能力等级规定。

8.5.2 主用、灾备中心之间存储系统 SAN 网络的互联链路带宽应符合同步/异步远程复制 要求，不宜小于 10Gbit/s。

8.6 应用级容灾

8.6.1 应用主备、应用双活容灾模式的灾难恢复性能不应低于《信息安全技术信息系统灾难恢复规范》GB/T 20988）中第 5 级、第 6 级灾难恢复能力等级的相关规定。

8.7 云桌面系统性能

8.7.1 桌面连接协议性能

8.7.1.1 正常办公场景下（非视频播放）虚拟机网络带宽占用不宜大于 1024Kbit/s。

8.7.1.2 为运营生产网业务应用服务的云桌面系统应支持丢包率不大于 0.01%，抖动时延不大于 10ms，单向时延不大于 30ms。

8.7.1.3 为内部管理、外部服务网业务应用服务的云桌面系统应支持丢包率不大于 0.1%， 抖动时延不大于 10ms，单向时延不大于 50ms。

8.7.2 虚拟桌面性能

8.7.2.1 虚拟桌面 vCPU 数量应支持 1~32 个。

8.7.2.2 虚拟机桌面内存应支持当 32bit 时 1~4GB，当 64bit 时 1~512GB。

8.7.3 云桌面管理系统性能

8.7.3.1 单套云桌面系统最大支持用户数不应小于 5000 个.

8.7.3.2 单套云桌面系统支持并发登录用户数不应小于 50 用户/秒。

8.8 云管理平台性能

8.8.1 云平台管理存储复制容灾应支持不少于 5000 虚拟机（含系统卷与数据卷）.

8.8.2 云管理平台可管理的数据中心数量不少于 16 个，可管理的物理机数量不少于 500 个，可管理的虚拟机数量不少于 10000 个。

8.8.3 云管理平台支持的服务目录数量不少于 200 个，支持同时在线用户数不少于 100 个。

8.9 智能运行平台性能

8.9.1 从数据进入大数据模块实时处理平台到处理完毕输出，应支持不高于 1s 的数据延迟。应支持关键字搜索的毫秒级响应。

8.9.2 大数据模块应具备良好的扩展性，可平滑扩展至 PB 级数据存储能力.

8.9.3 系统故障时，数据中断不应大于 20s，不应丢失任何历史数据.。

8.9.4 系统平台主备切换时间不应大于 3s。

9 网络安全要求

9.1 综合业务云平台应满足《信息安全技术 网络安全等级保护基本要求》GB/T 22239，并为各个业务系统的安全防护提供符合要求的网络安全服务，全量的系统日志至少存储 6 个月。

9.2 综合业务云平台应具备云安全防护管理功能，包括身份认证，安全接入，基础安全保障，云底层安全，云主机安全，云网络安全，应用安全，云数据安全等。

9.3 综合业务云平台应具备云安全运营管理功能，包括云资产识别，安全审计服务，安全运营服务，日志统一收集分析服务，云网流量分析服务，云安全仪表板服务等.

9.4 综合业务云平台应具备云安全调度管理功能，包括多云统一管理服务，混合云统一管理，跨云安全资源编排，跨平台多云资源监控能力等。

9.5 综合业务云平台的云安全管理应深度集成纳管上述各类别安全组件，需覆盖从远程接入、边界防护、入侵防护、病毒过滤、终端防护、堡垒机、数据库审计等全面的安全能力。

9.6 综合业务云平台应提供立体化的安全防护能力，满足各种合规标准中信息安全防护的要求。

9.7 综合业务云平台需支持实时展示主机安全防护状态、待处理风险、风险趋势以及主机安全的实时动态。

9.8 云平台应遵循“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。

9.9 云平台应按照网络安全等级保护三级建设，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。

9.10 应用系统部署在云平台上的部分，其安全措施应由应用系统自身安全机制和云平台安全机制协同保障，云平台应能根据应用系统需求统一提供安全计算环境、安全区域边界、安全通信网络及数据交换安全、入侵防范、虚拟层和平台层安全等，应用系统应保障自身计算环境、运行环境的安全。

9.11 云平台应具备开放接口或开放性安全服务，允许应用系统接入第三方安全产品，或可在云平台选择第三方安全服务。

9.12 云平台应保障云基础设施安全，确保虚拟化安全、通信网络安全、存储安全等。

9.13 云平台应具备架构安全的设计特点，应实现分层分区的安全架构，保障不同网络的隔离、不同专业应用和用户的隔离。

9.14 云平台应保证自身计算环境安全，具备身份鉴别、访问控制、安全审计、可信验证、数据完整性、数据保密性、数据备份恢复、剩余信息保护、个人信息保护等功能。

9.15 云平台应设置安全管理中心。

9.16 云平台内部网络终端设备应具备防病毒和终端管控能力，部署终端安全管理设备及终端防病毒设备。

9.17 云平台物理机、虚拟机应具备防病毒和终端管控能力，应根据终端特点及性能损耗部署终端安全管理设备及终端防病毒设备。

9.18 云平台应保障城际铁路云数据的本地备份与恢复，宜建立异地灾备中心，对重要数据进行实时异地备份，当发生安全事件后能迅速恢复，不影响业务正常运行。

9.19 云平台应为云上各应用系统提供自主设置安全策略的能力，应能够自主定义访问路径、选择安全组件、配置安全策略。

9.20 云平台应具备针对云内各业务系统需求提供安全资源池的能力。

9.21 安全资源池宜将安全能力平台化、服务化、自动化交付。

9.22 安全资源池宜在安全生产网、内部管理网、外部服务网中分别部署。

9.23 安全资源池由独立设置的安全组件组成，安全组件可采用 X86 物理服务器、虚拟机或一体机形态部署。

9.24 安全资源池可通过核心交换机连通云上业务系统提供安全服务，实现跨不同 VPC 网络的通信。

9.25 安全资源池应允许接入第三方安全产品，或可在云平台选择第三方安全服务，云计算平台安全应具备开放接口。

9.26 安全资源池的服务能力宜符合下列规定：

a) 能提供虚拟防火墙和虚拟日志审计设备；

b) 能提供虚拟负载均衡设备；

c) 能提供虚拟网络流量管控审计设备；

d) 能提供虚拟堡垒机设备；

e) 能提供虚拟漏洞扫描设备；

f) 能提供虚拟 Web 应用防火墙设备；

g) 能提供用户态势平台设备。

10 云平台接口

10.1安全生产网

10.1.1 安检系统

10.1.1.1 线网/线路中心级变电所安检系统中的非云化部署设备（如打印机等）可采用独立组网部署方式，与中心级云平台的物理接口界面宜位于中心级云平台外部接入区交换机外侧，接口类型宜为以太网接口。

10.1.1.2 站段级安检系统中的非云化部署设备可采用独立组网部署方式，与站段级云节点的物理接口界面宜位于站段级云节点汇聚交换机外侧，接口类型宜为以太网接口。

10.1.2 变电所智能监控系统

10.1.2.1 线网/线路中心级变电所智能监控系统中的非云化部署设备（如打印机等）可采用独立组网部署方式，与中心级云平台的物理接口界面宜位于中心级云平台外部接入区交换机外侧，接口类型宜为以太网接口。

10.1.2.2 站段级变电所智能监控系统中的非云化部署设备可采用独立组网部署方式，与站段级云节点的物理接口界面宜位于站段级云节点汇聚交换机外侧，接口类型宜为以太网接口。

10.1.3 车辆智能运维系统

车载子系统和地面数据处理平台之间应具备 WIFI 等无线通信方式，支持 TCP 或 UDP 传输协议。地面数据处理平台系统与非云化部署的业务系统（如无线通信等系统）之间，物理接口界面宜位于云平台外部接入区交换机外侧，接口类型宜为以太网接口。

10.1.4 乘客信息系统

10.1.4.1 线网/线路中心级系统接口应符合下列规定：

a) 中心级乘客信息系统中的非云化部署设备（如打印机等）可采用独立组网部署方式， 与中心级云平台的物理接口界面宜位于中心级云平台外部接入区交换机外侧，接口类型宜为以太网接口；

b) 中心级乘客信息系统与视频监视系统之间，物理接口界面宜位于中心级云平台外部接入区交换机或边界安全设备外侧，接口类型宜为以太网接口。

10.1.4.2 站段级乘客信息系统中的非云化部署设备（如控制器、显示屏等）可采用独立组网部署方式，与站段级云节点的物理接口界面宜位于站段级云节点汇聚交换机外侧，接口类型宜为以太网接口。

10.1.5 段场安防系统

段场安防系统中的非云化部署设备可采用独立组网部署方式，与站段级云节点的物理接口界面宜位于站段级云节点汇聚交换机外侧，接口类型宜为以太网接口。

10.1.6 轨道监测系统

10.1.6.1 线网/线路中心级轨道监测系统中的非云化部署设备（如打印机等）可采用独立组网部署方式，与中心级云平台的物理接口界面宜位于中心级云平台外部接入区交换机外侧，接口类型宜为以太网接口。

10.1.6.2 站段级轨道监测系统中的非云化部署设备可采用独立组网部署方式，与站段级云节点的物理接口界面宜位于站段级云节点汇聚交换机外侧，接口类型宜为以太网接口。

10.1.7 门禁系统

10.1.7.1 线网/线路中心级系统应符合下列规定：

a) 中心级门禁系统的非云化部署设备与云平台的接口位于中心级云平台外部接入区交换机外侧，接口类型宜为以太网接口；

b) 中心级门禁系统与非云化部署的业务系统之间，物理接口界面宜位于中心级云平台外部接入区交换机或边界安全设备外侧，接口类型宜为以太网接口。

10.1.8 票务及客服系统

10.1.8.1 中心级系统接口应符合下列规定：

a） 清分中心系统的非云化部署设备与中心级云平台的物理接口界面宜中心级云平台外部接入区交换机外侧，接口类型宜为以太网接口；

b） 线网客服系统中的非云化部署设备（如打印机等）可采用独立组网方式，与中心级云平台的物理接口界面宜位于中心级云平台外部接入区交换机外侧，接口类型宜为以太网接口。

10.1.8.2 车站级票务及客服系统中的非云化部署设备（如 TVM、BOM、AGM、紧急按钮控制器、客服自助终端等）应采用独立组网方式，与车站级云节点的物理接口界面宜位于车站级云节点汇聚交换机外侧，接口类型宜为以太网接口。

10.1.9 视频监视系统

10.1.9.1 线网/线路中心级视频监视系统的非云化部署设备（如编解码器、大屏幕显示系统等）宜采用独立组网部署方式，与中心级云平台的物理接口界面宜位于中心级云平台的外部接入区交换机外侧，接口类型宜为以太网接口。

10.1.9.2 站段级视频监视系统的非云化部署设备（如编解码器、监视器、本地存储设备等）宜采用独立组网部署方式，与站段级云节点的物理接口界面宜位于站段级云节点汇聚交换机外侧，接口类型宜为以太网接口。

10.1.10 信号运维保障系统

线网/线路中心级信号运维保障系统的非云化部署设备宜采用独立组网部署方式，与中心级云平台的物理接口界面宜位于中心级云平台的外部接入区交换机外侧，接口类型宜为以太网接口。

10.1.11 智能监测管理平台/通信集中告警系统

线网/线路中心级智能监测管理平台/通信集中告警系统的非云化部署设备宜采用独立组网部署方式，与中心级云平台的物理接口界面宜位于中心级云平台的外部接入区交换机外侧，接口类型宜为以太网接口。

10.1.12 综合监控系统/轨道交通综合管理指挥系统

10.1.12.1 线网/线路中心级系统应符合下列规定：

a） 中心级综合监控系统/轨道交通综合管理指挥系统的非云化部署设备（如大屏幕显示系统等）宜采用独立组网部署方式，与中心级云平台的物理接口界面宜位于中心级云平台的外部接入区交换机或边界安全设备外侧，接口类型宜为以太网接口；

b） 中心级综合监控系统与非云化部署的业务系统（如广播等）之间，物理接口界面宜位于中心级云平台外部接入区交换机或边界安全设备外侧，接口类型宜为以太网接口。

10.1.12.2 站段级系统接口应符合下列规定：

a） 站段级综合监控系统/轨道交通综合管理指挥系统的非云化部署设备（如通信前置机、打印机、IBP 盘等）宜采用独立组网部署方式，与站段级云节点的物理接口界面宜位于站段级云节点汇聚交换机外侧，接口类型宜为以太网接口；

b） 站段级综合监控系统与非云化部署的业务系统（如广播等）之间，物理接口界面宜位于站段级云节点汇聚交换机外侧，接口类型宜为以太网接口。

10.1.13 自动扶梯部件预警系统

10.1.13.1 线网/线路中心级自动扶梯部件预警系统中的非云化部署设备（如打印机等）可采用独立组网部署方式，与中心级云平台的物理接口界面宜位于中心级云平台外部接入区交换机外侧，接口类型宜为以太网接口。

10.1.13.2 站段级自动扶梯部件预警系统中的非云化部署设备可采用独立组网部署方式，与站段级云节点的物理接口界面宜位于站段级云节点汇聚交换机外侧，接口类型宜为以太网接口。

10.2内部管理网

10.2.1 内部管理信息系统宜采用中心级、站段级两级结构，系统全部均部署于中心级云平台和站段级云节点，与相关业务系统的接口应均为云平台承载应用系统之间的软件接口，接口界面在云平台内部。

10.2.2 内部管理信息系统均部署在综合业务云平台，与相关业务系统的接口应均为综合业务云平台所承载业务系统之间的软件接口，且接口界面在综合业务云平台内部。

10.3外部服务网

10.3.1 外部服务网系统全部部署于中心级云平台，由云平台承载应用系统间的软件接口，接口界面在云平台内部。

10.3.2 外部服务网系统通过安全隔离措施与互联网系统实现相关信息交互，接口类型宜为以太网接口。