ICS 33.060.99
CCS M 36

T/EJCCCSE

团　　体　　标　　准

T/EJCCCSE XXX—2024

5G 通信运维平台

5G communication operation and maintenance platform

（征求意见稿）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

2024－XX－XX 发布　　2024－XX－XX 实施

中国商业股份制企业经济联合会　　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这些专利的责任。

本文件由中国商业股份制企业经济联合会提出并归口。

本文件起草单位：苏州新奥图智能科技有限公司、江苏慧东出智能科技有限公司。

本文件主要起草人：宫雨 方刚　刘少辉。

本文件为首次制定。

5G 通信运维平台

1 范围

本文件规定了5G 通信运维平台的参考框架及安全要求。
本文件适用于5G 通信运维平台的设计和运行。

2 规范性引用文件

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

YD/T 3628 5G移动通信网 安全技术要求
YD/T 3807 移动通信网络设备安全保障通用要求

3 术语和定义

本文件没有需要界定的术语和定义。

4 缩略语

下列缩略语适用于本文件。
IaaS:基础设施即服务(Infrastructure-as-a-Service)
IPaaS:集成平台即服务(Integration Platform as a Service)
APaaS:应用平台即服务(Application Platform as a Service)
SaaS:软件即服务(Software-as-a-Service)
CMDB:配置管理数据库 Configuration Management Database)
ITIL:IT基础架构库(Information Technology Infrastructure Library)
DevOps:一组过程、方法与系统的统称(Development和Operations的组合)
OS:操作系统(Operating System)
Linux:操作系统
Windows: 美国微软公司研发的一套操作系统(Microsoft Windows)
AIX:基于AT&T Unix System UNIX操作系统(Advanced Interactive eXecutive)
Ksh:linux命令调用(Korn shell)
P2P:对等互联网络技术(Peer To Peer)
TCP:传输控制协议(Transmission Control Protocol)
Bash:环境变量(Bourne-Again Shel)
IDC:互联网数据中心(Internet Data Center)
SOA:面向服务的架构(Service-Oriented Architectur)
Cmd:命令提示符(cmd.exe)
Shell:命令行解释器(Shell)
Bat:批处理文件(Batch(bat)
Cygwin:UNIX模拟环境(Cygwin)
DataFlow:数据流图(Dataflowdiagram)
IBMCPU:中央处理器(Central Processing Unit)
DB:数据库(Database)
ESB:企业服务总线(Enterprise Service Bus)
KV:键值 (key value)

SDK：软件开发工具包（Software Development Kit）
SDN：软件定义网络（Software Defined Network）
API：应用程序接口（Application Programming Interface）
TSOB：数据表（data sheet）
Overlay：覆盖层（overburden）
Web：万维网（World Wide Web）

5 参考框架

5.1 框架组成

由IaaS管控层、通用组件层、PaaS层和运维场景层组成。每层定义如下：

a) IaaS 管控层：是指对 IaaS 层资源的管理和控制，通过提供指令、文件、数据下发的管道， 适配各类型操作系统和主机，并兼容私有云、公有云以及混合云的管理方式；
b) 通用组件层：是指为满足通用运维场景的基础能力平台的封装，由 CMDB 模块、作业功能模块、运维数据平台模块、容器管理模块、智能运维模块等功能模块组成；
c) APaaS 层：支持应用部署和运行的 APaaS 以及企业内部 SOA 集成的 IPaaS，通过企业服务总线和 API 网关对接共性组件层各平台的能力；
d) 运维场景层：是指基于 PaaS 层之上构建的运维 SaaS，涵盖基础运维、监控告警、ITIL 流程、DevOps、任务编排、弹性伸缩、安全审计等各领域。

5.2 IaaS 管控层

5.2.1 是整个云计算运维框架的底层支撑体系， 是上层运维场景与底层 IaaS 的连接器，为上层提供指令、文件、数据的通道，支持直连、代理以及为达到最优接指定级联路由方式的模式。

5.2.2 应采用分布式 C/S 架构，主要包含智能 Agent 和提供文件分发传输、命令实时执行、大数据采集与传输服务能力的服务器，及服务注册与发现、KV 存储、关系型数据库等模块，可支持私有云、公有云和混合云等多种异构架构，以及虚拟机、容器和各种 OS 等设备。

5.2.3 应支持私有云、公有云、混合云,IaaS 管控层应能够适配企业内 IDC、各类公有云的独立管控以及混合云的统一管控,具体为：

a) 对于企业内 IDC，应支持 Agent 直连模式管控；
b) 对于公有云管控，可通过设置 Agent 为代理模式，实现对该片区域云主机的管控；
c) 对于网络隔离区域的管控，具备设置指定级联路由的方式实现对其管控。

5.2.4 应支持虚拟机、容器以及各类 OS，应能够支持适配主流 Linux、Windows、AIX 版本以及对底层虚拟技术和容器的兼容。

5.2.5 应具备以下文件分发与传输功能：

a) 传输模式：
   1) 应支持大文件传输模式：指对于一定大小以上的文件分发自动启用大文件传输模式作为首选传输方式，提升文件的分发效率以及避免拥塞，如 P2P 模式；
   2) 应支持直传模式：指针对一定大小以下的文件使用直传模式，如 TCP 模式；
   3) 宜支持混合模式：指在大文件传输模式传输持续性失败，则会尝试使用直传模式传输大文件分片；当大文件传输模式恢复时，则停止直传模式。
b) 传输类型：
   1) 文件传输：是指将多种格式、可读目录下的单个文件分发到指定机器；文件分发完成后，自动同步目标文件权限与源文件一致；文件传输结束后进行文件完整性和一致性检查；
   2) 目录传输：用户将指定目录分发到多台机器指定可写目录下，目录分发将保持源目 录结构和权限不变；
   3) 正则匹配传输：用户通过通配符（符合通用正则规则）指定多个文件，并传输到指定机器的指定可写目录，传输完成后文件的格式和权限与源文件保持一致。
c) 传输控制：

1) 区域链控制：指通过设定规则，使文件只能在两个区域间单向传输，以满足具有特殊专线链接的两个区域间的传输需求；
2) 跨区域穿透：指原本相互隔离的两个区域需要进行文件传输，需对本次传输进行定向穿透。管控平台允许权限用户适当修改配置来完成这种定向穿透。

5.2.6 实时任务执行应包括任务类型和任务控制，具体定义如下：

a) 任务类型：
   1) 命令类型：Linux 支持 bash 命令、Windows 支持 cmd 命令、AIX 支持 ksh 命令，支持自定义可执行文件格式程序的启动，支持解释性语言程序的执行；
   2) 脚本类型：Linux 支持 Shell 脚本、Windows 支持 bat 脚本（安装有 Cygwin 的额外支持 Shell 脚本）、AIX 支持 ksh 脚本，以及各种系统支持的解释性脚本程序。
b) 任务控制：
   1) 指定用户：是指 Linux 及其他类 Linux 系统支持按指定用户执行任务；
   2) 继承用户环境：是指 Linux 及其他类 Linux 系统支持指定用户后继承该用户设定的环境变量；
   3) 是指用户选择校验机器密码，Windows Agent 按指定用户执行任务的功能；
   4) 有害操作告警：是指管控系统能够自动设定高危操作的定义，并支持对高危操作进行预警；
   5) 有害操作防护：管控系统能够自动识别高危操作，对高危操作进行预警和干预， 高危操作的定义及干预措施提供选项供用户配置。

5.2.7 数据采集与传输包括数据采集服务和集群管理两部分，具体定义如下：

a) 数据采集服务：
   1) 应支持自定义数据采集：Agent 开放数据发送接口、cmdline 及 SDK，提供用户开发自定义的数据采集程序或脚本；
   2) 应支持采集器插件化支持：Agent 支持采集器插件化，自动加载采集插件，并监控插件的存活状况。如果采集插件异常终止，则重新拉起采集插件；如果连续拉起失败超过 4 次则触发告警；
   3) 应支持实时数据快照：管控层支持缓存安装有 Agent 的机器 1 分钟内的快照数据，并提供接口供用户访问；
   4) 应支持动态负载均衡：由于 Agent 数据采集的量大，且具有随业务特性波动的特点，数据在流转时需要高性能的服务端做收敛转发，为提高服务端机器的利用率，减少由于数据量变化时带来的负载不均衡问题，管控系统支持按分钟级别动态调整数据转发的通道，以达到集群内服务端负载均衡的目的。
b) 集群管理:
   1) 应支持自动服务发现：管控平台同一个集群内的模块均支持自动发现，用户可以扩容、缩容任何节点，系统均能实时感知，并调整通讯策略，保证服务的高可用；
   2) 应支持集群负载均衡：管控平台同一个集群内，支持按照 Agent 链接数进行负载均衡；
   3) 应支持 Agent 状态查询：管控平台提供接口，查询 Agent 状态。
   4) 宜支持多区域负载均衡：管控平台支持对同一集群进行不同区域的划分,不同区域按照各区域内的负载均衡规则处理;未划分区域的 Agent 按照集群负载均衡策略处理。

5.3 通用组件层

5.3.1 CMDB 模块

包括业务层面的主机资源管理、业务拓扑资源管理、业务管理、自定义属性管理、进程端口与配置文件管理、对象管理、资源分组、数据审计和操作审计等功能。

5.3.1.1 主机资源管理

指管理基于业务层面的主机资源应支持拓扑维度的资源概况展示， 应支持外部资源的导入和云主机的实时同步，应支持跨云管理主机；对于不同类型业务的主机资源，宜支持具备自定义属性的扩展功能。

5.3.1.2 业务拓扑资源管理

业务拓扑资源是CMDB进行主机管理的基础，准确的业务模型将决定主机的结构化管理，CMDB需提供用户结构自定义、拓扑属性自定义等功能，可针对不同的场景选择性的建立与业务匹配的结构。

5.3.1.3 业务管理

应支持面向不同角色提供业务的权限级别管理和业务的增删改查等操作，运维操作平台的所有权限都以CMDB为核心。

5.3.1.4 自定义属性管理

CMDB提供自定义模型属性适配各类业务场景，用户可基于业务、集群、模块和主机等对象新增自定义属性，同时可关联主机自定义采集策略，实时下发采集策略到线上主机并上报数据到CMDB，供周边系统使用。

5.3.1.5 进程端口与配置文件管理

将业务的进程、端口、配置文件注册到CMDB，并关联到业务拓扑中，为上层应用如监控、 进程管理等提供数据和配置服务。

5.3.1.6 对象管理

可根据用户需求自定义管理的对象类型，新增的对象类型可关联到具体的业务拓扑， 也可以API方式提供对应的增删改查功能供周边系统使用。

5.3.1.7 资源分组

CMDB中提供静态数据与动态数据两种配置数据，资源分组功能可以结合动静态数据对资源进行任意组合，供周边系统使用。

5.3.1.8 数据审计

将动态数据与CMDB中的已存在静态数据进行周期性对比，当数据不一致时，进行告警并给出统一对比结果。

5.3.1.9 操作审计

用户在CMDB上的操作都有对应的记录可供追溯，并且所有操作审计记录都需录入到事件中心。

5.3.2 作业功能模块

5.3.2.1 作业功能模块是底层基于管控之上的基础运维操作平台，宜支持海量的并发处理能力，支持脚本执行、文件拉取/分发、定时执行等多种可实现的基础运维场景；支持将单个任务组装成一个作业流程，同时可通过平台提供的 API 实现对任意作业的调用、查看等操作；与其它平台或系统进行联动，实现调度自动化。

5.3.2.2 管控平台的 Agent 可触发作业平台的任务执行和文件传输，使用大文件传输方案应对较大文件的传输，如 P2P 模式，使得文件拉取和传输更高效。文件的拉取和传送更加便捷，可支持的“多对多、多对一” 的多模式文件分发传输任务。

5.3.2.3 云化脚本管理模式，应支持多个协作者通过平台进行脚本共享使用，同时可支持 Web 脚本单独执行和多个脚本或文件传输流程串接组合成作业任务。

5.3.2.4 针对运维场景中的多服务器操作应能够支持企业服务器管理规模扩大之后的并发执行任务能力。

5.3.2.5 应支持作业平台的文件传输、 脚本执行等共性组件步骤编排为作业流程，实现复杂场景下的自动化作业执行，以便后续的管理和复用。

5.3.3 运维数据平台模块

5.3.3.1 实现计算、存储、查询和分析的全流程自助化大数据服务。运维人员可以通过统一数据接入、可视化计算任务配置、可视化建模、 统一查询等功能，快速的构建基于大数据的可视化、智能化运维支撑工具。

5.3.3.2 统一数据接入提供了数据采集、数据汇聚、 数据清洗、数据传输的全自助化的服务， 目 标是最大化降低数据接入门槛、提升数据接入的效率和质量。用户无需登录服务器进行操作和故障排查，就可接入数据，数据类型包括：基础性能、组件日志、业务日志、DB 数据、自定义上报、HTTP 等。

5.3.3.3 DataFlow 是将业务运维数据的实时计算、离线计算、算法分析等一系列复杂数据处理相融合的一种计算方式，用户使用标准的 SQL 和拖拽功能就可以构建一个复杂的，多层级的混合计算逻辑。运维数据平台 DataFlow 是可以同时配置管理实时计算与离线计算，一份原始数据的整个处理流程可以在 DataFlow 中体现，用户可基于 DataFlow 进行实时、离线数据计算，数据过滤等复杂数据处理。

5.3.3.4 可视化建模流是将业务运维的数据分析挖掘低成本化，将机器学习算法共性组件节点化，将模型的构建过程标准化。用户可以按照标准流程通过拖拽配置共性组件节点，完成数据分析挖掘模型的构建，解决运维中的数据挖掘问题。可视化建模流与 DataFlow 深度集成，可视化建模流运行实例可以与实时计算、 离线计算组合成 DataFlow，完成了从构建到实例运行的整个闭环。

5.3.3.5 通常存储类型分为：关系型、KV 型、时序型、全文检索型和分析型，根据运维数据的类型（基础运维数据、时间序列数据、文本事件数据）、大小和使用场景，将运维数据分类存储。基础运维数据（运维元数据）使用关系型存储和 KV 型存储适用于运维信息明细查询;文本事件数据使用全文检索引擎；时间序列数据使用场景比较广泛，其中使用 TSDB 存储用于实时监控，使用分析型存储用于多维数据分析，以及使用离线存储用于历史数据的保存和归档

5.3.4 容器管理模块

5.3.4.1 包括应用仓库、容器编排和调度服务、多环境一致性管理、容器网络服务、容器安全服务以及监控一体化和日志查询服务。

5.3.4.2 包含用户所需的操作系统、运行时环境和应用程序的镜像仓库， 应支持部署集群或创建容器实例。应用仓库分为公开仓库和私有仓库，主要用于存放镜像。应用仓库对高可用以及安全有很高的要求，以保障镜像得到及时获取和分发。

5.3.4.3 容器云平台提供容器编排和调度服务， 应支持应用集群一键部署、云计算资源弹性扩展、 容器编排和自定义调度等功能，为用户提供了高性能的容器集群管理方案。 应支持弹性伸缩、垂直扩容、灰度升级、服务发现、服务编排、错误恢复、性能监测等功能，让应用能够快速部署服务。

5.3.4.4 容器技术实现了操作系统和硬件间的解耦，便于运维技术人员能及时发现不同系统间的差异，并根据这些差异进行调配，避免出现系统运行错误等情况。通过容器技术可提供有效的多环境一致性解决方案，保证开发、测试、生产环境的一致性，提高系统运行的稳定性。

5.3.4.5 容器管理平台需具备通过 SDN 网络，向虚拟机和容器提供统一的 overlay 网络，以及服务导出和负载均衡的功能。

5.3.4.6 容器管理平台支持冗余、自恢复、高可扩展模型并具备基础安全能力，结合安全基础防护、安全监测管理、安全运维等，形成完整的容器管理平台安全防护体系。

5.3.4.7 监控一体化功能应能够支持容器以及容器间通信进行自定义监控和展示，采用事前预警和事后报警的机制，保证应用可靠性，帮助运维人员快速发现、定位问题，并将应用从失效状态进行恢复，为应用的健康运行提供多方位的可靠性保证。容器日志的统一查询服务，可帮助运维根据不同的日志维度定位应用程序问题以及进行日志查询。

5.3.5 智能运维模块

智能运维模块是指在运维领域能够提供数据分析挖掘服务，主要目标是降低运维领域数据分析挖掘的门槛。能够提供拖拽式建模、交互式测试调优、自动化模型评估、模型训练运行管理、 场景模型（公共的通用的模型）等功能，包含了从模型构建评估到模型发布管理整个的功能链路，通过将各种基础的数据挖掘、机器学习算法节点化，将模型构建的过程标准化，将数据分析挖掘工作简单化。

5.4 APaaS 层

5.4.1 是一个开放的平台层，包含用于支持用户简单快速的创建、部署和托管应用的 APaaS，以及提供了完善的前后台开发框架、服务总线（ESB）、调度引擎、公共组件等模块的 IPaaS，为一个应用从创建到部署，再到后续的维护管理提供了完善的自助化和自动化服务，如日志查询、监控告警等。
5.4.2 运维平台 PaaS 层提供支持多语言的开发框架，平台之上支持 Python、php 等技术语言开发运维自动化工具。开发框架集成统一登录鉴权模块、功能开关模块、WEB 安全防护模块、功能组件模块等通用模块。
5.4.3 应用运维平台 PaaS 层提供从 SaaS 的创建、 部署以及维护管理均实现免运维托管服务。 首先通过运维平台开发的 SaaS 工具在平台采用分布式部署方式，可一键自动部署；SaaS 部署使用 Docker 进行隔离，提高 SaaS 安全性；开发者可通过平台日志查看功能来使用日志记录和日志监控告警服务，并可以自定义配置相应的告警参数、告警接收人等信息，实时监控日志数据。
5.4.4 运维平台 PaaS 层提供 SaaS 运营数据管理功能， 运维人员需增强对运营数据的使用价值， 包括其用户访问量、在线时长，活跃度等指标，平台可综合展示 SaaS 的使用情况。同时针对应用的 Docker 容器所占用内存和 CPU 进行实时监控统计， 供用户了解应用的 CPU 和内存使用情况。
5.4.5 运维平台 PaaS 层提供企业服务总线或 API 网关功能， 对作业功能模块、CMDB、数据平台、 容器管理模块等共性组件平台统一开放 API 以组件形式进行统一和集中化管理， 以及对共性组件的权限校验、频率控制、访问统计、路由分发以及自助接入等功能，上层应用场景统一通过企业服务总线&API 网关调用组件 API。

5.5 运维场景层

5.5.1 运维场景层是基于 PaaS 之上快速构建应用场景 SaaS 的面向运维场景解决方案的载体。 通过对底层平台能力共性组件功能的拼装实现基础运维、CI/CD、监控告警、任务编排、 弹性伸缩、安全审计以及移动运维等各类场景的自动化。
5.5.2 针对运维工作中的日志查看、数值调整、数据提取、性能展示、配置变更等基础运维的自动化。
5.5.3 针对代码集成、构建、检查、测试、部署、缺陷管理以及版本管理，实现全链路的自动化和可视化。
5.5.4 实现主机性能、日志、自定义属性、应用性能、公共组件以及调用链等指标的监控告警， 并能针对有确定处理流程的告警实现故障自愈。
5.5.5 基于共性组件的封装和编排，并支持共性组件的自助开发接入，实现各异构平台间的无缝连接，解决运维场景操作全流程的调度自动化。
5.5.6 根据容量、负载评估以及在线预测等智能决策模型，实现无人值守的弹性伸缩。
5.5.7 针对运维日常操作的高危扫描、行为监控、审计对帐，实现运维操作记录和操作结果的可追溯性。
5.5.8 将部分简易固化的临时操作以及信息通知在移动端呈现，并可通过即时通讯工具的上下行实现部分交互的执行。

6 安全要求

6.1 5G 移动通信网安全技术应符合 YD/T 3628 的规定。5G 移动通信网络设备安全应符合 YD/T 3807 的规定。
6.2 入网安全验收应包含以下内容:

a) 检查设备是否存在无主账号、默认账号；
b) 检查设备是否已对系统的端口和服务等基础安全信息进行备案；
c) 检查各分层是否具备相关日志记录功能，是否对日志访问设置了权限；
d) 检查登录设备口令设置的复杂度是否合适；
e) 适用评估工具对系统和网络进行安全扫描，查找是否存在漏洞；
f) 检查是否已经安装了指定授权的防病毒软件，病毒库是否已更新至最新。
g) 检查网元业务流程和通信协议是否存在漏洞。

6.3 数据安全应符合以下要求：

a） 应做好数据的分级分类管理、数据访问权限管理；
b） 应做好数据的操作行为管理；
c） 应制定数据采集、传输、存储、使用、共享和销毁等环节的安全管控措施；
d） 应制定数据安全应急预案；
e） 应做好安全补丁管理，定期进行漏洞扫描。对干无补丁的漏洞，应有访问控制策略，并不定期进行安全监测；
f） 应建立完善的数据备份与恢复机制，定期执行灾难备份恢复能力检测，更新备份关健数据；
g） 应使用安全的随机数生成器产生公私密钥对，并对私钥进行加密存储和备份。禁止私钥以明文形式导出专用密码设备；
h） 应支持周期性检查证书是否过期或即将过期，并对已过期或即将过期证书进行提醒；
i） 应定期检查合规配置，包括操作系统，数据库等；
j） 应按规定将安全日志、安全事件通过接口统一上报，进行集中化的安全监测及告警处置。