

团 体 标 准

T/CSNAME 130—2026

船舶大数据岸基综合监控管理平台技术要求

Technical requirements for ship big data shore-based integrated monitoring and management platform

2026 - 10 - 10 发布

2027 - 01 - 10 实施

中国造船工程学会 发 布

目 次

前言 III

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 缩略语 1

5 组成和功能 2

 5.1 计算资源 2

 5.2 存储资源 3

 5.3 网络资源 3

 5.4 信息资源 4

 5.5 应用支撑 5

 5.6 服务交付 6

 5.7 互联互通 7

 5.8 时钟管理 7

 5.9 数据管理 8

6 机房设施要求 10

 6.1 机房环境 10

 6.2 机房基础设施 10

 6.3 供配电要求 10

 6.4 机房空间与安全域 10

 6.5 通信线路要求 10

7 性能要求 10

 7.1 平台响应时间 10

 7.2 启动时间 11

 7.3 迁移时间 11

 7.4 存储性能 11

 7.5 网络性能 11

 7.6 信息交换性能 11

8 测试要求 11

 8.1 功能测试 11

 8.2 性能测试 12

 8.3 安全测试 12

 8.4 兼容性测试 12

 8.5 故障恢复测试 12

 8.6 运维与更新测试 12

 8.7 网络连接性测试 13

 8.8 时钟管理测试 13

8.9 测试报告 13



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。

本文件由中国造船工程学会船舶标准化专业委员会提出。

本文件由中国造船工程学会归口。

本文件起草单位：中国船舶集团有限公司第七一一研究所、齐耀能效（上海）科技有限公司、大连海事大学。

本文件主要起草人：张呈龙、刘青林、史斌杰、王洋、王伟铭、石浩舰、江川、王付双、唐慧妍、姜瑞政。



船舶大数据岸基综合监控管理平台技术要求

1 范围

本文件规定了船舶大数据岸基综合监控管理平台(以下简称综合监控管理平台)的架构、性能要求、功能要求及运维测试要求。

本文件适用于船舶大数据岸基综合监控管理平台的设计、开发、应用和测试。

2 规范性引用文件

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

GB/T 32908—2016 非结构化数据访问接口规范

GB 50174 数据中心设计规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

船舶大数据岸基综合监控管理平台 ship big data shore-based integrated monitoring and management platform

部署于岸基,基于船岸通信获取船舶相关数据,利用大数据技术对数据进行采集、汇聚、存储、分析、展示和管理的平台化系统。

4 缩略语

下列缩略语适用于本文件。

AIS——自动识别系统 (Automatic Identification System)

AMQP——高级消息队列协议 (Advanced Message Queuing Protocol)

API——应用程序编程接口 (Application Programming Interface)

BGP——边界网关协议 (Border Gateway Protocol)

CIFS——通用互联网文件系统 (Common Internet File System)

GIS——地理信息系统 (Geographic Information System)

HTTPS——超文本传输安全协议 (Hypertext Transfer Protocol Secure)

IP——网络之间互连的协议 (Internet Protocol)

LZ4——基于 LZ77 的压缩算法 (LZ77-based Compression Algorithm)

MQTT——消息队列遥测传输协议 (Message Queuing Telemetry Transport)

NFS——网络文件系统 (Network File System)

OGC——开放地理空间信息联盟 (Open Geospatial Consortium)

OSPF——开放式最短路径优先 (Open Shortest Path First)

PB——数据存储单位拍字节 (Petabyte)

PUE——电源使用效率 (Power Usage Effectiveness)

SFTP——安全文件传输协议 (SSH File Transfer Protocol)

SIFT——尺度不变特征变换 (Scale-Invariant Feature Transform)

SMB——服务器消息块协议 (Server Message Block)

TF-IDF——词频-逆向文件频率 (Term Frequency-Inverse Document Frequency)

TLS——传输层安全协议 (Transport Layer Security)

VPN——虚拟专用网络（Virtual Private Network）

5 组成和功能

综合监控管理平台基本组成和功能架构见图1。

监控管理平台应能提供计算资源服务、存储资源服务、网络资源服务、信息资源服务、应用支撑服务、服务受理交付服务、互联互通服务、时钟管理服务等功能。



图1 船舶大数据岸基综合监控管理平台组成和功能

5.1 计算资源

5.1.1 主机资源管理

平台应支持对主机的统一接入、配置、运行及资源管理，包括但不限于以下功能：

- a) 支持将已配置的物理主机添加至公共平台；
- b) 支持从公共平台中删除物理主机；
- c) 支持禁用或启用主机部署功能；
- d) 支持对主机执行远程开机和关机操作；
- e) 支持设置主机负载均衡策略；
- f) 支持将主机添加至主机资源池；
- g) 支持从主机资源池中删除主机。

5.1.2 虚拟机资源管理

平台应支持对系统映像、虚拟机资源及虚拟机运行状态的统一管理，包括但不限于以下功能：

- a) 支持制作系统映像模板，并支持系统映像、光盘映像及数据盘映像的添加和删除；
- b) 支持单台或批量添加、部署虚拟机，并支持自动和手动部署模式；
- c) 支持根据虚拟机配置，从映像池、网络池和存储池中分配相应的映像、网络及存储资源；
- d) 支持基于系统映像或光盘映像创建和部署虚拟机；

- e) 支持虚拟机资源的释放、回收及重新分配;
- f) 支持在释放计算资源后重建和删除虚拟机,并保持虚拟机原有配置不变;
- g) 支持虚拟机的启动、关闭、重启、挂起、休眠及恢复;
- h) 支持虚拟机快照的创建、保存、恢复和删除,并支持通过快照实现虚拟机运行状态的备份与恢复。

5.1.3 动态资源调度

平台应支持对虚拟机计算、存储等资源的动态分配,包括但不限于以下功能:

- a) 支持根据虚拟机运行状态及故障情况,自动执行虚拟机在线迁移;
- b) 支持计算资源超配、资源限额及弹性负载管理;
- c) 支持对关机状态的虚拟机进行系统配置;
- d) 支持虚拟机配置编辑,并按照编辑后的新配置运行虚拟机;
- e) 支持计算资源分级管理;
- f) 支持对运行中的虚拟机进行磁盘空间动态扩容;
- g) 支持对运行中的虚拟机动态增加磁盘资源。

5.2 存储资源

5.2.1 存储资源管理

平台应支持对存储资源的创建、扩展、调度、虚拟化及数据迁移管理,包括但不限于以下功能:

- a) 支持创建存储资源,并支持采用多种类型的磁盘创建存储资源;
- b) 支持存储资源的动态扩展,并支持存储集群的动态扩展;
- c) 支持存储资源的弹性调度和自动分配;
- d) 支持通过设置存储卷共享方式,对存储卷的访问用户进行指定和管理;
- e) 支持对不同品牌、型号的存储设备进行统一虚拟化管理;
- f) 支持对异构存储系统进行虚拟化,并支持虚拟化后的数据清理、数据整合、数据迁移及远程镜像复制;
- g) 支持不同类型存储介质之间的数据双向动态迁移;
- h) 支持多种类型的存储接口及相应通信协议。

5.2.2 存储资源维护

平台应支持对存储系统的统一配置、运行监控、故障管理及维护升级,包括但不限于以下功能:

- a) 支持采用图形化管理界面对存储资源进行统一管理,并支持多种管理语言;
- b) 支持对存储资源使用情况、关键服务状态等运行信息进行统计与分析;
- c) 支持对存储设备进行实时运行状态监控,并提供设备异常报警功能;
- d) 支持存储系统自动部署,包括软件安装、配置及初始化,并支持即插即用;
- e) 支持存储设备及相关组件的热插拔;
- f) 支持在不中断业务系统运行的情况下,自动检测、定位并隔离存储系统故障;
- g) 支持存储系统的软件及相关组件自动升级。

5.2.3 存储数据管理

平台应支持对存储数据的统一管理,包括但不限于以下功能:

- a) 支持存储数据的导入和导出;
- b) 支持在存储数据传输过程中保持数据的完整性、一致性和高可用性;
- c) 支持存储数据保护,并提供快照、恢复、备份、复制、镜像及克隆等数据保护功能;
- d) 支持核心数据本地保存1年以上。

5.3 网络资源

网络资源服务功能包括网络资源管理、网络资源分配、网络分区管理等功能。

5.3.1 网络资源管理

平台应支持对网络资源的动态调度与管理，包括但不限于以下功能：

- a) 支持基于云计算技术实现网络资源池的动态调度；
- b) 支持核心交换机采用虚拟集群技术，实现核心网络设备的冗余；
- c) 支持接入交换机采用堆叠技术，实现接入网络设备的冗余；
- d) 支持核心交换机与接入交换机之间采用链路捆绑技术，实现链路冗余；

5.3.2 网络资源分配

平台应支持虚拟机网络资源的配置、分配、调度及接入管理，包括但不限于以下功能：

- a) 支持为虚拟机分配网络资源，并支持指定网络地址分配和随机网络地址分配；
- b) 支持虚拟网络标记及虚拟机网络网段划分；
- c) 支持根据组织机构动态分配 VPN 服务，为用户提供公共平台网络接入能力，并支持 VPN 服务的统一监管；
- d) 支持采用软件化、模块化和组件化方式提供 VPN 服务；
- e) 支持网络设备扩展，并支持为单台虚拟机配置多个网络；
- f) 支持网络资源的自动化和弹性管理；
- g) 支持弹性公网 IP 地址分配；
- h) 支持公网 IP 地址与指定虚拟机之间的绑定和解绑。

5.3.3 网络分区管理

平台应支持网络资源的分区、隔离及安全防护，包括但不限于以下功能：

- a) 支持按照业务功能对公共平台核心网络进行逻辑隔离；
- b) 支持将公共平台网络划分为管理域、业务域和存储域，并支持不同网络域之间的物理隔离；
- c) 支持对公共平台内部网络及各区域设置独立的网络平面和业务区域；
- d) 支持按照安全组或安全域对各网络区域进行划分，并支持基于安全域实现网络资源的逻辑隔离及安全防护。

5.4 信息资源

信息资源服务功能包括信息资源目录体系服务、信息资源交换体系服务、信息资源服务发布、数据融合服务、数据仓库服务、数据挖掘服务和数据比对服务等功能。

5.4.1 信息资源目录体系服务

平台应支持信息资源目录的编目、分类、发布、检索及授权管理，包括但不限于以下功能：

- a) 支持信息资源目录的审核、编目和发布；
- b) 支持按照资源类型、业务类别等对信息资源目录进行分类管理；
- c) 支持信息资源目录及资源内容的检索，并支持快速定位目标资源；
- d) 支持信息资源目录的分级授权管理；

5.4.2 信息资源交换体系服务

平台应支持不同业务系统之间的信息资源交换、协议适配、数据传输及交换过程监控，包括但不限于以下功能：

- a) 支持部署于公共平台上的不同业务系统之间进行数据交换，并支持对数据交换过程进行监控和管理；支持 JSON、XML、CSV、Parquet、Avro 等结构化数据，Syslog、Log4j 等半结构化数据，以及 JPG、PNG 图片、MP4、AVI 视频、WAV、MP3 音频、PDF、DOCX 文档等非结构化数据，以及 NMEA 0183、NMEA 2000、S57、S63、AIS 报文等船舶专用格式数据的交换；
- b) 支持多种数据交换及通信协议，包括 HTTP/HTTPS (RESTful API)、MQTT、AMQP、FTP/SFTP、WebSocket、NFS、CIFS、SMB 等，以适应船岸通信、窄带卫星通信、边缘节点及文件共享等不同通信场景；
- c) 支持数据传输过程中的加密及压缩处理，包括 TLS 等传输加密机制和 LZ4 等数据压缩格式；
- d) 支持断点续传、数据缓存及传输队列管理。

5.4.3 信息资源服务发布

平台应支持信息资源服务的发布、管理及授权调用，包括但不限于以下功能：

- a) 支持发布可被授权用户受控调用的信息资源服务接口，并支持服务接口的统一管理；
- b) 支持将信息资源快速封装并发布为服务；
- c) 支持与信息资源目录体系集成，将已发布的信息资源服务纳入信息资源服务接口目录统一管理；
- d) 支持根据用户角色及访问权限实施分级授权，为不同用户提供差异化的服务访问和调用权限。

5.4.4 数据融合服务

平台应支持多源异构数据的融合、处理、发布及二次开发，包括但不限于以下功能：

- a) 支持航海日志、船舶姿态、航速航向、雷达图像、AIS 数据、气象海况等船舶专有数据的融合、叠加及处理，并提供数据查询和分析能力；
- b) 支持融合数据服务的发布，并支持 OGC 标准服务接口；
- c) 支持提供多种二次开发接口及服务接口，并支持用户根据业务需求自主选择开发工具；
- d) 支持 GIS 数据与其他业务数据进行融合，并提供数据查询、空间定位等功能。

5.4.5 数据仓库服务

平台应支持数据仓库及数据集市的创建、管理、处理和服务能力，包括但不限于以下功能：

- a) 支持数据仓库和数据集市的创建、配置及统一管理；
- b) 支持数据清洗、数据装载、数据查询及数据展现；
- c) 支持面向不同用户提供多实例数据仓库服务，并实现实例的独立管理。

5.4.6 数据挖掘服务

平台应支持数据在线分析、报表展现、数据挖掘及安全权限管理，包括但不限于以下功能：

- a) 支持提供数据仓库配置管理、数据建模及报表展现设计工具，并支持主流关系型数据库管理系统及数据文件；
- b) 支持以表格、饼图、柱状图、仪表盘等形式进行分析结果展示，并支持基于瘦客户端实现数据过滤、分组、计算等灵活分析功能及报表导出；
- c) 支持单点登录及统一门户功能，并支持将报表分析结果集成至业务系统；支持提供多用户共享且可独立使用的数据挖掘服务；
- d) 支持集中式安全控制及权限继承机制，根据用户角色、组织及授权范围实施差异化的信息访问权限管理。

5.4.7 数据比对服务

平台应支持数据预处理、数据比对及比对结果管理，包括但不限于以下功能：

- a) 支持配置多个预处理任务和数据比对任务，并支持对参与处理的表及字段进行灵活配置；
- b) 支持多个预处理任务和数据比对任务并行执行，并支持手动和自动两种任务执行方式；
- c) 支持灵活配置预处理流程、比对流程及数据比对规则；
- d) 支持严格的事务控制机制，保证数据处理过程中的完整性和一致性，并支持预处理及比对结果以报表形式输出；
- e) 支持主流关系型数据库管理系统。

5.5 应用支撑

5.5.1 构件服务管理

平台应支持软件构件的统一存储、开发、部署及运行管理，包括但不限于以下功能：

- a) 支持构件仓库的分类管理和版本管理，并支持构件的上传、下载及检索；
- b) 支持开发工具与构件仓库对接，实现构件的上传、下载，并支持开发程序打包、代码编译与测试以及预置开发模板；
- c) 支持对通过开发工具打包的应用系统进行运行支撑和部署管理；
- d) 支持服务构件的热加载，实现服务构件的动态加载及即插即用。

5.5.2 软件服务化封装

平台应支持工具软件的服务化封装、权限控制、访问隔离及运行监控，包括但不限于以下功能：

- a) 支持用户权限与数据权限分离，实现不同用户之间的数据访问隔离，保证用户仅能访问和操作授权范围内的数据；
- b) 支持隐藏软件服务化封装后的实际服务地址，防止用户绕过监控管理平台直接访问工具软件；
- c) 支持单实例及多实例工具软件的服务化封装与接入；
- d) 支持用户使用权限的分配和回收，并支持根据业务需求灵活配置用户访问授权时间；
- e) 支持对服务化封装的工具软件进行服务进程监控，实时掌握服务运行状态。

5.5.3 应用 API 的提供(接口)

平台应支持开放性API接口的提供、访问控制、安全认证及调用管理，包括但不限于以下功能：

- a) 支持提供开放性 API 接口，并支持 XML、WebService 等接口形式；支持 OAuth 2.0、Token、API Key 等主流身份认证机制，并结合用户角色按照最小权限原则实施接口访问授权；
- b) 支持 API 通信采用 HTTPS 协议进行加密传输；在公网传输或船岸通信存在中转节点的场景下，支持采用 TLS 1.2 及以上版本的加密标准；
- c) 支持对外部系统接入实施 IP 白名单、接口访问频率及调用次数等控制措施，防止恶意调用、非法访问及接口滥用；
- d) 支持自动记录 API 接口调用日志，日志至少包含调用方身份、调用时间、接口路径、响应状态等信息，并支持异常调用的统一响应及报警通知。

5.5.4 监控管理平台预置服务构件的要求

平台应支持预置服务构件的统一提供、发布、管理及运行支撑，包括但不限于以下功能：

- a) 支持提供服务受理与交付类服务构件，实现服务发布、申请、审批、交付、管理及监控等功能；
- b) 支持提供信息资源类服务构件，包括信息资源目录系统、数据交换系统、多元数据融合系统、基础资源公共服务系统、数据比对系统、数据挖掘系统及大数据处理系统等；
- c) 支持提供安全及运维类服务构件，包括数据库加密引擎池系统、虚拟机防护系统、软件 VPN 系统、统一用户管理及单点登录系统、跨域身份认证系统、运行监控系统及运维流程管理系统等服务构件。

5.6 服务交付

5.6.1 服务发布

平台应支持服务的创建、发布、配置、审批及全生命周期管理，包括但不限于以下功能：

- a) 支持公共监控管理平台服务的创建和发布；
- b) 支持对上传的服务插件进行服务项配置、插件上传及插件基本信息录入；
- c) 支持对服务插件进行分类查询、信息编辑及信息查看；
- d) 支持对服务资源信息进行审批、查看、检索、挂起、关闭、恢复、审计及状态控制；
- e) 支持新发布服务的热加载，实现服务的动态加载和即时生效。

5.6.2 服务受理

平台应支持服务资源的申请、审核、开通及续约管理，包括但不限于以下功能：

- a) 支持用户提交服务资源申请，并形成服务资源申请订单；
- b) 支持管理员对服务资源申请订单进行审核，并对审核结果进行管理；
- c) 支持服务资源的开通，申请订单审核通过后，按照申请内容向用户分配相应服务资源；
- d) 支持服务资源续约，服务到期后用户可提交续约申请及续约订单，并由管理员进行审核，审核通过后继续向用户提供相应服务资源。

5.6.3 服务交付实施

平台应支持服务资源的交付、使用管理及服务实例访问，包括但不限于以下功能：

- a) 支持服务资源交付申请，并支持服务资源的挂起、关闭及释放；

- b) 支持第三方服务供应商自主集成并发布自有服务；
- c) 支持根据服务申请自动或手动完成资源的创建、分配、绑定及释放；
- d) 支持已申请服务实例的单个登录。

5.6.4 服务交付管理

平台应支持服务资源的运行管理、分类管理、服务评价、统计分析及订购审批，包括但不限于以下功能：

- a) 支持对处于不同运行状态的服务插件进行统一管理；
- b) 支持用户对服务进行评价，并支持客户建议与投诉提交、受理及满意度反馈；
- c) 支持服务资源的分类查询、分类添加、分类删除及分类管理；
- d) 支持服务量统计，能够按照指定时间段对服务资源使用情况及服务订购信息进行统计分析；
- e) 支持服务提供商自定义服务规范及服务订阅策略；
- f) 支持管理员对服务订购过程进行审批及权限管理。

5.7 互联互通

5.7.1 统一身份认证

平台应支持用户统一身份认证、权限管理及跨平台访问控制，包括但不限于以下功能：

- a) 支持多个监控管理平台之间的用户统一身份认证及合法访问控制；
- b) 支持通过平台端和客户端进行用户登录，并支持用户身份及相关数据同步；
- c) 支持对用户身份和访问权限进行统一认证与授权；
- d) 支持监控管理平台内部及跨平台访问的单个登录；
- e) 支持用户名和口令、证书 Key、动态密码等身份认证方式，并支持上述认证方式的组合使用。

5.7.2 统一运维管理

平台应支持运行状态监测、故障事件管理及业务应用运行监控，包括但不限于以下功能：

- a) 支持公共监控管理平台运维故障事件的发现、记录、处理及闭环管理；
- b) 支持按照平台层级分级采集公共平台运行状态数据，并支持多级平台自动上报运行状态数据；
- c) 支持对运行于公共平台上的业务应用进行运行状态监测，并支持相关业务系统管理方对业务应用运行状况进行统一管理。

5.7.3 数据交换

平台应支持监控管理平台之间的数据交换及安全控制，包括但不限于以下功能：

- a) 支持多个监控管理平台之间的数据交换，并支持基于最短路径的数据交换；
- b) 支持对数据交换过程实施身份认证和访问授权；
- c) 支持对数据交换结果实施访问控制。

5.8 时钟管理

5.8.1 统一时钟服务

平台应支持统一时钟服务，包括但不限于以下功能：

- a) 支持为平台各业务模块、数据采集服务及日志服务提供统一的系统时间基准；
- b) 支持系统时间的初始化、校准和维护，确保平台各模块的时间基准一致。

5.8.2 时间同步与冗余切换

平台应支持时间同步及冗余切换，包括但不限于以下功能：

- a) 支持标准时间同步协议，并支持根据应用需求配置时间同步参数；
- b) 支持配置主、备时间服务器，并在主时钟源不可用或通信中断时，自动切换至备用时钟源；
- c) 支持在时钟源恢复后重新建立时间同步，并对时钟源切换过程及同步状态进行记录。

5.8.3 时钟状态监测与异常告警

平台应支持时钟状态监测与异常告警，包括但不限于以下功能：

- a) 支持监测时钟同步状态、时间偏差及时间同步服务运行状态；
- b) 支持配置时间偏差阈值，并在时钟同步异常、时间漂移超限或发生非预期时间回拨时生成日志并触发报警；
- c) 支持查询时钟异常事件的发生时间、异常类型、持续时间及处理状态。

5.8.4 时间一致性管理

平台应支持时间一致性管理，包括但不限于以下功能：

- a) 支持在数据对账、日志合并及故障回溯等场景下，识别不同数据源或系统之间的时间戳不一致情况；
- b) 支持对时间戳异常的数据进行标记，并根据业务规则提供时间戳修正或异常提示功能。

5.9 数据管理

5.9.1 存储与计算设施

平台应支持多类型计算与存储设施的配置、扩展及数据缓存管理，包括但不限于以下功能：

- a) 支持磁盘、磁盘阵列、内存存储、键值存储、关系型存储、分布式文件系统等一种或多种存储设施；
- b) 支持单机、并行计算集群、分布式计算集群等一种或多种计算设施；
- c) 支持船舶长期海上作业场景下的离线数据缓存及自动补传；
- d) 支持数据存储硬件的扩展，满足数据存储容量及处理能力的持续扩展需求。

5.9.2 存储管理

平台应支持数据存储建模、存储实例管理、数据操作及存储能力扩展，包括但不限于以下功能：

- a) 支持涵盖原始数据、基本属性、底层特征及语义特征的概念层存储建模，并支持逻辑层存储建模；
- b) 支持整型、浮点型、布尔型、字符串、日期、日期时间、二进制块等基本数据类型，以及向量、矩阵、关联等数据类型；
- c) 支持根据逻辑层存储模型创建存储实例，并支持对存储实例进行数据插入、修改和删除，以及删除存储实例；
- d) 支持非结构化数据操作的原子性；
- e) 支持全局事务定义，并保证事务的原子性、一致性、隔离性和持久性；
- f) 支持数据类型的多值结构和层次结构；
- g) 支持在不同存储设施上创建存储实例，并实现存储实例与底层存储设施的自动映射；
- h) 支持 PB 级数据存储。

5.9.3 特征抽取

平台应支持从非结构化数据中抽取名称、类型、创建者、创建时间等基本属性，并支持从文本、图像、音频、视频中至少一种非结构化数据中进行特征抽取；

- a) 支持文本特征抽取，包括词、停用词、TF-IDF 特征及关键词等文本特征；
- b) 支持图像特征抽取，包括颜色空间、主导颜色、色彩内容、颜色结构、颜色布局等颜色特征，以及均匀纹理、边缘直方图等纹理特征和区域形状、轮廓形状等形状特征；
- c) 支持音频特征抽取，包括基于静音检测提取有效音频片段，以及音频波谱、MFCC 等音频特征；
- d) 支持视频特征抽取，包括按照镜头抽取视频片段及抽取视频关键帧。

5.9.4 特征抽取扩展要求

平台应支持多类型非结构化数据的特征抽取及语义分析，包括但不限于以下功能：

- a) 支持文本特征扩展抽取，包括人名、地名、机构名、时间等实体信息，以及主题词、摘要和语义特征；

- b) 支持图像特征扩展抽取, 包括 SIFT 局部区域描述特征和语义特征;
- c) 支持音频特征扩展抽取, 包括音频指纹、旋律、音色、响度及语义特征;
- d) 支持视频特征扩展抽取, 包括运动特征和语义特征。

5.9.5 索引管理

平台应支持索引的创建、维护、删除及大规模数据索引管理, 包括但不限于以下功能:

- a) 支持索引的建立、维护和删除;
- b) 支持 B+树索引、倒排索引、全文索引及高维索引等多种索引类型;
- c) 支持 PB 级数据索引。

5.9.6 查询处理

平台应支持多类型数据查询、查询结果处理及大规模数据检索, 包括但不限于以下功能:

- d) 支持范围查询、全文查询、样例查询、语义查询及跨媒体查询等多种查询方式;
- e) 支持对查询结果进行相关性排序, 并支持查询结果批量返回;
- f) 支持查询相关性反馈功能, 根据用户反馈优化查询结果的相关性;
- g) 支持 PB 级数据查询。

5.9.7 访问接口

应符合GB/T32908—2016中4~6章规定的查询语言访问接口要求。

5.9.8 管理工具

平台应支持数据管理及系统运维相关工具的统一提供, 包括但不限于以下功能:

- a) 提供安装部署工具;
- b) 提供逻辑层模型定义工具;
- c) 提供查询分析工具;
- d) 提供任务管理工具。

5.9.9 转换加载

平台应支持多类型非结构化数据的格式转换及加载, 包括但不限于以下功能:

- a) 支持常用格式的文本数据转换及加载;
- b) 支持常用格式的图像数据转换及加载;
- c) 支持常用格式的音频数据转换及加载;
- d) 支持常用格式的视频数据转换及加载;
- e) 支持提供面向特定应用领域的非结构化数据转换及加载工具集。

5.9.10 分析挖掘

平台应支持数据分析与数据挖掘模型的定义、执行及工具集管理, 包括但不限于以下功能:

- a) 应支持分析模型定义;
- b) 应支持分析模型执行;
- c) 应支持挖掘模型定义;
- d) 应支持挖掘模型执行;
- e) 应提供数据挖掘工具集。

5.9.11 可视展现

平台应支持多类型数据的可视化展示及可视化分析, 包括但不限于以下功能:

- a) 支持文本、图像、音频及视频等多类型数据的可视化展现;
- b) 支持提供柱状图、折线图及饼图等常用可视化方法;
- c) 支持提供标签云、关系图等扩展可视化方法;
- d) 支持提供基于地图的可视化方法, 实现数据与地理空间信息的关联展示。

5.9.12 统计信息

平台应支持系统运行性能及资源容量的统计分析，包括但不限于以下功能：

- a) 支持系统平均数据插入时间的统计，并提供相应统计信息；
- b) 支持系统平均查询响应时间的统计，并提供相应统计信息；
- c) 支持系统可支撑的数据量及数据存储容量的统计，并提供相应统计信息；
- d) 支持系统可支撑的并发用户数统计，并提供相应统计信息。

6 机房设施要求

6.1 机房环境

平台机房环境应满足以下指标：

- a) 机房内温度范围宜为 18℃~27℃，相对湿度不宜大于 60%；
- b) 改造的旧机房 PUE 不应超过 2，新建机房 PUE 不应超过 1.5。PUE 为数据中心总能源消耗与 IT 负载能源消耗的比值。

6.2 机房基础设施

机房的分级要求、建筑条件要求、配套设施要求、布线要求、配电要求、不间断电源要求、新风空调区和消防设施区都应符合GB50174—2017中选址及设备布置、环境、建筑与结构、网络与布线、电气、电磁屏蔽、空气调节、消防安全等要求。

6.3 供配电要求

机房供配电系统应满足以下要求：

- a) 机房应配备 2 路来自不同配电板的电源且配备 UPS。
- b) 电源、空调、网络等关键设备应采取冗余配置，避免因单点故障影响机房正常运行。

6.4 机房空间与安全域

机房空间及安全域划分应满足以下要求：

- a) 公共平台核心机房应与平台管理边界之外的外部机房保持物理空间隔离；对于公共平台内承载不同业务或服务不同用户的机房区域，应根据业务独立性、用户需求及安全要求，设置独立的物理区域或采取相应的隔离措施；
- b) 应根据公共平台核心机房的功能、业务承载需求及安全要求划分安全域，明确各安全域的功能、边界及访问控制要求，保证不同安全域内的操作和管理相互独立；
- c) 安全域应同时采用逻辑划分和物理划分方式，并保持逻辑区域与物理区域的一致性；
- d) 安全区域至少包括网络接入区、业务开展区、安全服务区和调试区等。

6.5 通信线路要求

机房应支持多运营商通信线路接入，并支持不同运营商线路从不同物理位置进入机房。

7 性能要求

7.1 平台响应时间

监控管理平台的响应时间应符合表1的要求。

表1 船舶大数据岸基综合监控管理平台响应时间要求

序号	类别	指标内容	性能要求
1	应用操作	静态页面加载、基础数据查询等简单应用	≤3 s
2		涉及一定数据处理的分页查询、图表展示、数据统计等一般应用	≤10 s
3		多源数据融合、大数据分析、复杂图形渲染等复杂应用	≤30 s
4	信息交换	局域网内单笔信息交换	≤10 s
5		局域网外单笔信息交换	≤40 s

表1 船舶大数据岸基综合监控管理平台响应时间要求（续）

序号	类别	指标内容	性能要求
6	交换监控	日志查询响应时间	≤ 3 s
7		交换服务、适配器运行状态响应时间	≤ 15 s
8	服务接口与资源	WEBSERVICE 调用时间	≤ 3 s
9		服务资源列表检索	≤ 3 s
10		在线申请服务可用性	24 小时在线

7.2 启动时间

虚拟机部署启动时间应满足以下要求：

- 基于系统映像部署虚拟机时，单台虚拟机从开始部署至交付并启动运行的时间应小于 20 min；
- 基于光盘映像部署虚拟机时，单台虚拟机从开始部署至交付并启动运行的时间应小于 1 h。

7.3 迁移时间

在物理机轻负载情况下，虚拟机完成在线迁移时间应小于 30 s，虚拟机完成离线迁移时间应小于 60 s。

7.4 存储性能

存储系统的性能及容量应满足不同业务场景下的数据处理和持续存储需求，包括以下要求：

- 在多种数据块大小混合读写条件下，存储系统 IOPS 应不小于 100,000，读写带宽应不低于 10 GB/s，平均响应时间应小于 30 ms；
- 对常见文件系统进行读写操作时，存储系统每秒操作数（IOPS）应不低于 100,000；
- 应根据船型规模及数据接入频率配置存储资源，基础可用存储容量应不低于 500 TB，并支持按需弹性扩容；
- 应按月对存储系统容量进行监测，当实际存储使用率超过 70% 时，应及时增加存储资源。

7.5 网络性能

网络系统的性能应满足平台业务运行和数据传输需求，包括以下要求：

- 外部接入网络带宽速率应达到千兆级别，内部网络带宽速率应达到千兆或万兆级别以上；
- 虚拟网络资源服务准备时间应不超过 20 min，光链路配置生效时间应不超过 20 min；
- 内部网络最大端到端延迟时间应小于 100 ms，丢包率应小于 0.5‰；
- 内部网络防火墙吞吐量应不低于 100 Gbps；
- 内部网络交换机交换容量应不低于 16 Tbps，包转发率应不低于 9600 Mpps；
- 应按月对核心路由器出口链路带宽进行监测，当实际带宽使用率超过 70% 时，应评估并实施链路扩容。

7.6 信息交换性能

信息交换服务的处理能力及并发能力应满足多业务场景下的数据交换需求，包括以下要求：

- 数据交换服务适配器运行环境单次加载的适配器实例数应不少于 100 个；
- 单次支持的数据交换记录数应不少于 2000 条；
- 单次公文交换应支持 20 MB 以内的公文数据
- 数据交换服务适配器运行环境支持的并发数应不少于 50 个。

8 测试要求

8.1 功能测试

采用黑盒测试方法设计测试用例，覆盖监控管理平台各项关键功能，验证系统功能实现的完整性、正确性、稳定性及运行效率，包括但不限于以下测试内容：

- a) 计算资源测试：验证主机管理、虚拟机管理及动态资源调度功能，包括主机添加、删除、启用/禁用，虚拟机部署、资源释放、在线迁移、负载均衡及磁盘动态扩容等操作，验证相关功能的正确性及运行稳定性；
- b) 存储资源测试：验证存储资源的创建、扩展、调度、虚拟化及数据迁移功能，检查存储资源管理、维护及数据保护功能的正确性，重点验证快照、备份、恢复等功能的有效性及数据完整性；
- c) 网络资源测试：验证网络资源动态调度、虚拟机网络资源分配、VPN 服务管理及网络分区隔离功能，检查网络设备及链路冗余、网络弹性、资源调度及安全隔离功能的稳定性和有效性；
- d) 数据管理测试：验证磁盘、内存存储、分布式文件系统等多类型存储设施的数据管理能力，检查数据存储、计算、索引管理、查询处理及 API 接口等功能在大规模数据场景下的性能和稳定性，并验证文本、图像、音频、视频等数据的可视化展现效果。

8.2 性能测试

使用性能测试工具进行测试，收集并分析测试结果，评估监控管理平台在高负载下的响应能力、吞吐量、资源利用率等性能指标。具体测试内容如下：

- a) 平台响应时间测试：模拟不同并发用户数进行简单、一般、复杂应用的请求，验证请求响应时间是否符合要求。
- b) 机房环境测试：在规定的温度和湿度范围内测试设备的稳定性，验证机房 PUE 值是否满足要求。
- c) 虚拟机部署与迁移：测试虚拟机从部署到交付运行的时间，在线迁移时间和离线迁移时间。
- d) 存储性能测试：测试系统在混合读写情况下的 IOPS、带宽、平均响应时间，以及存储系统的扩容能力。
- e) 网络性能测试：测试外部接入带宽、内部网络带宽、端到端延迟、丢包率、防火墙吞吐量、交换容量等，确保满足性能要求。
- f) 信息资源交换性能测试：测试数据交换服务适配器的加载能力、交换记录支持、信息交换时效。

8.3 安全测试

结合自动化工具与人工渗透测试，全面评估监控管理平台安全性，防范潜在的安全威胁。具体测试内容如下：

- a) 漏洞扫描：使用安全扫描工具检测监控管理平台存在的安全漏洞。
- b) 渗透测试：模拟黑客攻击，测试监控管理平台的安全防护能力。
- c) 数据加密与传输安全：验证数据加密算法的强度、数据传输过程中的安全性。
- d) 审计与日志管理：检查系统日志的完整性、可追溯性及审计功能的有效性。

8.4 兼容性测试

采用仿真环境或物理硬件设备，逐一测试并记录结果，确保监控管理平台在不同浏览器、操作系统及硬件设备上均能正常运行。具体测试内容如下：

- a) 浏览器兼容性：测试监控管理平台在不同浏览器上的显示效果和功能。
- b) 操作系统兼容性：验证监控管理平台在不同操作系统上的兼容性。
- c) 硬件设备兼容性：检查监控管理平台在不同硬件设备上的运行状况。

8.5 故障恢复测试

结合实际场景设计故障模拟方案，记录恢复过程及结果，验证监控管理平台在发生故障时的恢复能力和数据保护机制。具体测试内容如下：

- a) 单点故障恢复：模拟单一组件（如服务器、数据库等）故障，测试系统能否自动或手动恢复。
- b) 数据备份与恢复：验证数据备份的完整性和恢复过程的可靠性。
- c) 灾难恢复演练：模拟重大灾难场景，测试整个系统的灾难恢复能力。

8.6 运维与更新测试

为保障监控管理平台在部署后具备良好的可维护性与可升级性，平台应具备以下运维能力，并对其进行测试验证：

- a) 平台维护模式测试：验证监控管理平台是否支持从运行模式平滑切换至维护模式，确保维护期间不中断核心业务服务；测试是否支持对部分功能模块热插拔、暂停、重启等操作，不影响其他模块运行；测试维护模式开启时，是否可向用户发布公告，并限制非授权用户的操作权限。
- b) 软件更新机制测试：验证平台是否支持软件版本识别、历史版本回退及兼容性校验；测试是否支持在不中断服务的前提下进行微服务组件升级或重部署；测试是否支持关键安全补丁的发布、验证和快速生效机制；验证更新过程中是否记录完整操作日志，确保运维过程可追溯。
- c) 异常回滚与容灾切换：模拟更新中断、失败等情况，测试系统是否能自动或手动恢复到上一个稳定版本；验证在更新或维护期间出现系统崩溃，平台是否能切换至备用节点，保障业务连续性。

8.7 网络连接性测试

为确保监控管理平台在复杂通信环境下具备良好的联通能力与容错机制，应对网络连接性开展以下测试：

- a) 网络链路接入测试：验证平台是否能自动识别并接入多种通信链路；测试在主链路中断后，系统是否能自动切换至备用链路并保持服务不中断。
- b) 船岸通信测试：验证船岸之间的数据能否双向传输，并保持状态一致；模拟通信中断/恢复场景，验证平台是否能自动完成断点续传，确保数据完整性。
- c) 网络安全通道测试：测试平台是否可通过 VPN 建立加密通道进行远程访问与指令交互；测试系统是否能检测非法接入行为，并进行阻断或报警。

8.8 时钟管理测试

为确保平台中各类操作具备统一、准确的时间标记，应对系统时钟同步机制与管理能力进行以下测试：

- a) 时钟源接入测试：测试平台是否可识别有效时钟源，并将其作为系统时间参考。
- b) 时间同步准确性测试：对比多模块时间戳，验证时间偏差是否得到有效控制；断网状态下长时间运行平台，检测时间漂移是否在有效范围内。
- c) 时钟异常处理测试：模拟主时钟服务故障，验证平台是否可自动切换至备用时钟源；手动回拨系统时间，验证平台是否识别异常并触发告警。
- d) 日志与审计一致性测试：检查各系统日志、审计记录中的时间戳，验证其时序是否一致；对比来自不同子模块的数据记录时间，验证其时间戳一致性是否满足审计要求。

8.9 测试报告

测试报告内容应包括测试环境、测试过程、测试结果、问题记录及修复情况等。