

团 体 标 准

T/CSNAME 063—2022

船用设备远程运维数据管理要求

Data management requirements for remote operation and maintenance of marine equipment

2022-11-30 发布

2023-02-28 实施

中国造船工程学会 发 布

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提出并归口。

本文件起草单位：上海船舶运输科学研究所、中远海运能源运输股份有限公司、武汉船用机械有限责任公司、上海外高桥造船有限公司、武汉理工大学。

本文件主要起草人：韩冰、吴中岱、徐卫东、文逸彦、俞伯正、李飒、顾洪彬、柳师捷、范爱龙。



引 言

船用设备智能集成与远程运维标准群由13项标准组成，涵盖了船用设备智能集成模块设计、搭建、应用、维护等全过程，对该类问题有较好的指导作用。根据各项标准特点，本群标准所涉及的内容可分为以下四类：

——基础共性标准，包含《船用设备智能集成与远程运维通则》《船用设备标识编码要求》《船用设备智能集成可靠性设计要求》3项标准，可为后续内容提供整体性的指导。

——系统集成标准，包含《船用设备智能集成原则与要求》《船用设备信息集成平台通用技术要求》《船用设备远程运维系统接入要求》3项标准，对船用设备智能集成系统的搭建提出了要求。

——维护保养标准，包含《船用设备远程运维系统技术要求》《船用设备智能集成与远程运维系统 第1部分：状态监测》《船用设备智能集成与远程运维系统 第2部分：健康管理》《船用设备智能集成与远程运维系统 第3部分：视情维护》《船用设备智能集成与远程运维系统 第4部分：虚拟运维》5项标准，为船用设备智能集成系统的运行维护提供指导。

——数据管理与应用标准，包含《船用设备远程运维数据管理要求》《船用设备智能集成与远程运维系统 第5部分：知识库建设要求》2项标准，规范了系统所测数据的采集与处理方式。



船用设备远程运维数据管理要求

1 范围

本文件规定了船用设备远程运维的数据定义与范围、数据分类、数据采集与存储、数据集成与服务、数据及数据库管理、数据质量与安全等方面的一般要求与规范。

本文件适用于船用设备远程运维系统的开发与应用。

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 36344-2018 信息技术 数据质量评价指标

CB/T 4146-2011 船用计算机及外设 船用环境适用基本准则

ISO 16425 船舶和海洋技术舷侧设备和系统用船舶通信网络装置导则（Ships and marine technology — Guidelines for the installation of ship communication networks for shipboard equipment and systems）

CECS 72:97 建筑与建筑群综合布线系统工程设计规范（Code for engineering design of generic cabling system for building and campus revised edition）

中国船级社. 智能船舶规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

数据分类 data classification

将具有某种共同属性或特征的数据归并在一起，通过其类别的属性或特征来对数据进行区别。

3.2

数据质量 data quality

在指定条件下使用时，数据的特性满足明确的和隐含的要求的程度。

3.3

平台 platform

能够按需提供应用程序部署、管理和运行的操作环境。

3.4

结构化数据 structured data

一种数据表示形式，按此种形式，由数据元素汇集而成的每个记录的结构都是一致的并且可以使用关系模型予以有效描述。

3.5

非结构化数据 unstructured data

不具有预定义模型或未以预定义方式组织的数据。

4 船用设备运维数据分类

4.1 分类原则

船用设备运维数据依据以下原则进行分类：

- a) 稳定性原则：依据分类的目的，通过衡量数据波动性与离散性，选择船舶设备稳定的本质特性作为分类的基础和依据，以确保由此产生的分类结果能稳定的支持应用目标。在分类时，首先应明确界定分类对象稳定、本质的特征。
- b) 系统性原则：将选定的船舶设备特征（或特性）按其内在规律系统化进行排列，形成一个逻辑层次清晰、结构合理、类目明确的分类体系。
- c) 可扩充性：在类目的设置或层级的划分上，留有适当的余地，以保证分类对象增加时，不会影响已经建立的分类体系。
- d) 综合实用性：从实际需求出发，综合数据类型、来源等因素来确定具体的分类原则，使得由此产生的分类结果总体符合需求、综合实用和便于操作。
- e) 兼容性：与现行标准规定的分类原则相兼容。

4.2 分类方式

船舶设备运维数据可按以下方式进行分类：

- a) 按照设备运维数据物理属性分类，可分为感知数据、认知数据、控制数据、决策数据等。
- b) 按照设备运维场景分类，可分为面向船舶设备状态监测的数据、面向船舶设备故障诊断的数据、面向船舶设备健康管理的数据、面向船用设备视情维护的数据。
- c) 按照船端运维与远程运维数据分类，可分为船端运维数据、船端储存处理数据、岸端运维数据等。

5 数据存储与数据库管理

5.1 数据采集与接入要求

船端数据服务器应通过传感器或数据采集设备从船舶各个子系统采集数据，依照相关行业标准或协商标准接入数据服务器。

5.2 数据存储要求

- 5.2.1 船端数据服务器应能够存储输入数据不少于 30 天。
- 5.2.2 船端数据服务器应配备用户手册或安装手册，并提供每条记录存储空间大小的指南，以及总存储容量的信息。
- 5.2.3 船端数据服务器应协助用户估计船载数据服务器的总存储容量是否满足需求。

注：船端数据服务器可能具有冗余功能，以保护管理数据和实际记录的数据（如RAID 1、3和5系统）。

5.3 数据库物理环境安全管理

- 5.3.1 数据库所在的服务器、存储器等设备所处物理环境的温度、湿度、通风、防水、防尘、防雷、防震、防静电等应满足计算机机房的规范要求，机房环境、电源及防雷接地应满足 CECS 72:97 的要求。
- 5.3.2 数据库服务器应置于单独区域，任何物理访问都应获得授权或受到控制。

5.4 数据库操作系统运行维护管理

- 5.4.1 数据库操作系统不应提供任何其他如文件传输协议（File Transfer protocol, FTP）、域名服务（Domain Name System, DNS）等网络服务。
- 5.4.2 数据库操作系统应设置用于访问本地数据的专用账户，该账户具有除运行各项数据库服务以外的最低权限。
- 5.4.3 外界请求使用业务数据时，应向收集、存储、处理数据的数据库管理部门提出申请，经审批后由数据库管理员进行操作获取所需数据。

6 船端运维数据集成与服务

6.1 船端数据集成

船舶运维数据应来自于船上各个子系统，如压载水系统、货运系统、设备监测系统。船端数据服务器将船舶运维数据集成于船端数据管理平台，并与岸端数据平台保持通信及数据传输。

6.2 船端数据流动路径与服务

从设备端收集到所需的压载、货运、监测报警、环境监测及IBS等系统数据后，设备端数据通过数据流的形式输入船端数据集成管理平台，并存入船端数据服务器，监测报警、非振动类数据、振动类特征数据（基频、振动幅值）等通过数据流传输服务、请求—响应传输服务和文件传输服务三种形式输出至岸端数据平台，用以在岸端实现对船用设备的机电状态监测、故障分析、远程维护等等。

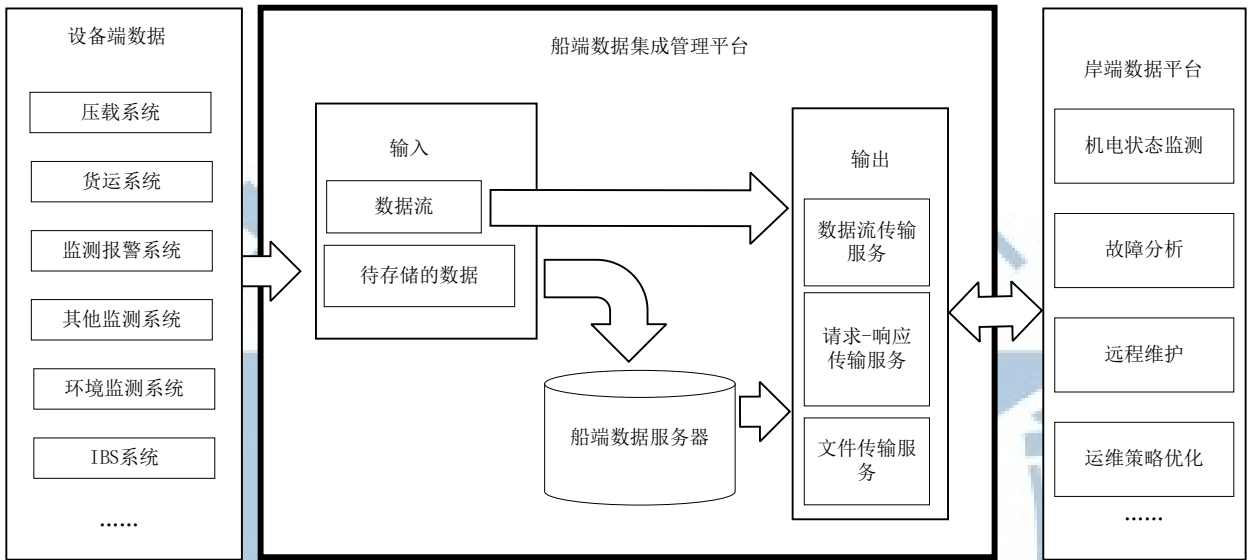


图1 数据流动路径示意图

7 岸端运维数据集成与服务

7.1 岸端数据集成

岸端数据平台接收来自船端数据集成管理平台发送的结构化数据与非结构化数据，集成于岸端数据平台，如图1所示。

7.2 岸端数据处理与服务

岸端数据平台通过对接收到的结构化数据与非结构化数据进行统一分析处理，实现基于认知运维数据基础之上的船端设备状态的监测，进而向船端提供重要机电设备的监测、故障分析、远程维护及运维策略优化等服务，船端数据集成管理平台接收到岸端数据，做出正确的指令，从而实现两端数据的交互，如图1所示。

8 数据质量与安全

8.1 基本原则

为保障获取到的船舶运维数据的质量及安全，数据管理主体应在组织整体业务活动和风险的环境下建立、实施、运作、监控、评审、维护和改进文件化的数据质量与安全管理体系。

8.2 数据质量评价指标

数据应满足 GB/T 36344-2018 中第 5 章要求。

8.3 网络安全要求

8.3.1 一般要求

船端数据服务器应安装在符合ISO 16425中6.1.1要求的网络内。

8.3.2 控制措施

网络安全控制措施应确保网络充分的管理和控制,以防范威胁、保护使用网络的系统和应用维护安全,包括传输的信息,包含以下内容:

- a) 制订明确安全策略;
- b) 建立安全组织;
- c) 实施网络资产分类控制;
- d) 加强人员安全管理;
- e) 保证物理实体和环境安全;
- f) 加强安全通信运行;
- g) 采取访问控制机制;
- h) 进行安全系统开发与维护;
- i) 保证业务持续运行;
- j) 遵循法律法规;
- k) 安全目标一致性检查。

8.3.3 网络服务安全

船上数据服务器应识别所有网络服务的安全特性、服务级别和管理要求,并包括在网络服务协议中,无论网络服务是内部提供还是外包。

8.4 本地安全要求

8.4.1 物理处所要求

计算机设备存放应符合CB/T 4146-2011中6.1条要求。正常失电时仍需使用的网络系统,应在正常供电失电时自动转接到备用电源。备用电源可采用不间断电源,其容量至少能维持30 min供电的需要。

8.4.2 物理访问控制

8.4.2.1 服务器型设备应位于可正常锁闭的房间内,以防止未经授权的访问。如条件不允许,设备应位于可锁闭的柜子或控制台内。

8.4.2.2 船舶网络主干网中的网络设备(路由器、交换机、防火墙、网关、协议转换器等)应安装在被保护的防火、防水的安全设施内。

8.4.2.3 当使用移动设备或便携式存储设备时,应符合以下要求:

- a) 除非经过特别授权,移动设备或便携式存储设备不应连接任何设备;
- b) 当便携式存储设备用于软件维护时,应在使用前经负责人授权;
- c) 除非连接外部设备进行维护或类似操作,到网络的连接应物理阻断;
- d) 应通过策略和物理或逻辑手段防止不适当和未经授权的便携式设备连接到系统的行为。

8.4.2.4 应通过以下入口控制手段对安全区域进行保护,如专人值守、安装屏障或配置电子门禁系统,以允许被授权人进入:

- a) 应配备访问记录表,记录访问者进入和离开区域的日期和时间,尤其是系统集成商或供应商的服务工程师等访问者,应通过身份证等进行认证,并且只允许授权的访问;
- b) 所有访问记录均应进行安全维护和监控。
- c) 物理安全设备(例如监视摄像机、入侵检测器、电子锁等)应具有强登录认证方法,如密码、智能卡、令牌等;如果采用密码,则应为非默认值,保持密码的复杂性,并定期更新;
- d) 物理安全设备应定期进行测试,确保其工作在正常作业状态;
- e) 物理安全设备的记录数据,应经授权才可进行维护和访问。

8.4.2.5 建立系统资产(包括设备、系统、工作站、服务器、可编程逻辑控制器、网络协议转换器、网络连接等)访问控制列表,并保持最新。

8.4.2.6 通过USB端口访问系统前,应对该端口传输的设备和/或数据进行检测。

8.4.3 设备安装部署

- 8.4.3.1 保障船舶网络及相关系统稳定运行的冗余设备应安装在不同房间或设备柜中。
- 8.4.3.2 当船舶主干网布线采取冗余形式时，冗余线缆应互相远离，例如从左右两舷分开铺设。
- 8.4.3.3 连接到系统的关键计算机和网络设备应安装在安全区域，包括边界接入域、计算域、网络基础设施域、支撑设施域，以避免外来者访问。

