

团 体 标 准

T/CSNAME 185—2026

绿色智能船舶协同研发平台数据安全 管理指南

Guidelines for data security management for green intelligent ship collaborative
R&D platform

2026 - 10 - 23 发布

2027 - 01 - 23 实施

中国造船工程学会 发 布

目 次

前言 1

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 安全需求 1

 4.1 保密性要求 1

 4.2 可用性要求 1

 4.3 完整性要求 1

 4.4 可控性要求 2

 4.5 不可否认性要求 2

5 数据分级 2

6 风险评估 2

 6.1 概述 2

 6.2 资产识别 2

 6.3 威胁识别 2

 6.4 脆弱性识别 3

 6.5 已有安全措施确认 3

 6.6 风险分析 3

 6.7 风险处置 3

7 组织管理要求 3

 7.1 安全组织与职责 3

 7.2 事件应急与演练 3

 7.3 第三方服务商安全管理 3

8 技术要求 3

 8.1 数据采集安全要求 4

 8.2 数据存储安全要求 4

 8.3 数据处理安全要求 4

 8.4 数据分发安全要求 4

 8.5 数据共享安全要求 5

 8.6 数据删除安全要求 5

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：中国船级社、水上载运装备安全研究院（宁波）有限公司、上海船舶运输科学研究所有限公司。

本文件主要起草人：邓林义、张旋武、乔继潘、刘桢、陈景昊、郭安康、任东隼、阮佳佳。



绿色智能船舶协同研发平台数据安全指南

1 范围

本文件规定了绿色智能船舶协同研发平台的数据安全需求、数据分级、数据安全风险评估、数据安全组织管理以及数据全生命周期的安全技术要求。

本文件适用于绿色智能船舶协同研发平台数据安全。

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 20984 - 2022 信息安全技术 信息安全风险评估方法

GB/T 35274 - 2023 信息安全技术 大数据服务安全能力要求

GB/T 37973 - 2019 信息安全技术 大数据安全管理指南

GB/T 43697 - 2024 数据安全技术 数据分类分级规则

GB/T 45577 - 2025 数据安全技术 数据安全风险评估方法

中国船级社，船舶数据质量评估指南，2021

中国船级社，船舶网络安全指南，2025

3 术语和定义

本文件没有需要界定的术语和定义。

4 安全需求

本平台数据安全应从保密性、可用性、完整性、可控性、不可否认性五个维度提出安全需求。

4.1 保密性要求

平台为保障研发数据不被未授权泄露，应满足下列保密性要求：

- 密钥的分配可采用人工和自动相结合的方式：密钥的产生和检验工作应由专门的密钥管理部门和授权的人员负责，密钥存储要按照国家有关规定，确保密钥的机密性、完整性和认证性。
- 应根据所传输或存储的科学数据安全分级和信息特征，确定对科学数据加密保护的方式（传输数据的用户加密、线路加密、存储数据的局部或全部加密、数据库内或库外加密等）。
- 应对传导和辐射产生的电磁信号泄露进行有效的抑制和屏蔽，以保证数据在一定范围内不被泄露。

4.2 可用性要求

为保障授权用户能够可靠访问平台合法数据资源，应满足下列可用性要求：

- 应确保授权用户经鉴别身份后允许进入系统。
- 应采用访问控制机制来保证合法用户只能访问与其身份相适应的数据资源。
- 应对访问数据资源的有关事件和有关操作进行安全审计，以便获得完整的记录，根据记录进行安全性的分析，并及时采取处理措施。

4.3 完整性要求

为保障平台研发数据、平台自身功能不被篡改、损坏，应满足下列完整性要求：

- a) 应对绿色智能船舶协同研发平台数据进行完整性检验；应定期检查存储数据媒介的物理损伤情况，尽量减少误操作、软件故障、硬件故障和强电磁干扰等意外事件，以保证数据的完整性。
- b) 应对绿色智能船舶协同研发平台确认其功能的正确性；为了防止被非法复制，应有唯一的标识，且能检验这种标识是否存在，以及是否被绕过；为了防止被非法修改，应具有抗分析能力和完整性检验的手段，安全防护要求可参照 CCS GD027 - 2025 第二章执行。

4.4 可控性要求

为实现对平台资源、数据、程序版本的全流程管控，应满足下列可控性要求：

- a) 应具备访问权限控制的管理机制。
- b) 应验证对绿色智能船舶协同研发平台协同资源和数据的访问、操作和使用的权限。
- c) 应验证平台、固件和配置文件的升级、加载和安装的权限。
- d) 应对接入平台的软件、固件和配置文件进行安全测试。

4.5 不可否认性要求

为实现数据收发行为可追溯、行为不可抵赖，应满足下列不可否认性要求：

- a) 应具有在请求的情况下，为数据发送方提供数据原发证据的功能；数据发送方不能否认发过数据，不能诬陷收方伪造数据。
- b) 应具有在请求的情况下，为数据接收者提供数据接收证据的功能，数据接收方能证实数据是由确认的数据发送方发来的，内容是真实的，对收到的数据不能修改和抵赖。

5 数据分级

本平台应依据数据发生泄露、篡改、损毁、非法获取、非法使用、非法共享后，对国家安全、经济运行、社会秩序、公共利益、组织权益、个人权益产生的危害程度，按照 GB/T 43697-2024 中 6.2 的要求开展平台数据分级。

完成数据分级后，应将分级标识附加至对应数据对象，按照分级结果实施差异化安全管控。平台一般数据按照本文件全部要求实施管理。

6 风险评估

6.1 概述

本平台宜结合 GB/T 20984-2022 第 5 章开展信息安全风险评估，并结合 GB/T 45577-2025 第 5 章开展专项的数据安全风险评估。风险评估包含资产识别、威胁识别、脆弱性识别、已有安全措施确认、风险分析、风险处置完整流程。

6.2 资产识别

针对绿色智能船舶协同研发平台开展数据资产识别时，应关注协同研发平台的特点，包括但不限于：

- a) 平台处理的个人信息；
- b) 平台的重要和核心、一般数据；
- c) 平台算法与软件；
- d) 平台数据基础设施；
- e) 平台协同业务机制；
- f) 平台数据存储框架，如分布式文件系统、非关系型数据库等；
- g) 平台数据平台计算资源（CPU、内存、网络等）管理框架等。

6.3 威胁识别

开展威胁识别时，应关注绿色智能船舶协同研发平台运行环境下的威胁特点，包括但不限于：

- a) 潜在攻击主体相关要素：攻击方资源、技术能力、动机；窃取、滥用数据的意图；访问处理数据所需资源；直接窃取访问数据的风险；攻击行为的成本收益；

- b) 恶意攻击所需专业知识与技能：数据分析所需专业技能、设备；利用系统脆弱性需要的技术知识；
- c) 数据出境带来的安全威胁。

6.4 脆弱性识别

开展脆弱性识别时，应关注绿色智能船舶协同研发平台运行环境下的脆弱性特定，包括但不限于：

- a) 数据存储、处理等基础软件和基础设施的脆弱性；
- b) 数据相关系统的脆弱性。

6.5 已有安全措施确认

应对已采取的安全措施的有效性进行确认。安全措施的选择可以参考CCS GD027-2025第4章要求。

6.6 风险分析

应选用合适方法与工具，判定威胁利用脆弱性触发安全事件的发生可能性；结合资产价值、脆弱性严重程度，综合研判安全事件发生后对国家安全、社会公共利益、组织及个人利益造成的损失与影响。

6.7 风险处置

根据风险分析结果确定风险处置策略，可选择风险规避、风险降低、风险转移、风险接受等处置方式，并形成风险评估报告，输出安全整改措施。

7 组织管理要求

7.1 安全组织与职责

组织应将平台数据安全纳入组织整体架构；明确平台数据安全责任主体、内部职责分工、汇报机制，指定专门的数据安全负责人。

7.2 事件应急与演练

组织应在应急预案和响应流程中明确平台发生数据泄露、篡改等安全事件的处置流程，包含监测、预警、处置、复盘各环节；应制定平台数据安全专项应急预案演练要求与通报机制，按组织制度定期开展演练。

7.3 第三方服务商安全管理

当平台业务引入第三方服务商时，应将服务商纳入安全管理流程。针对外包数据处理业务（如云服务、数据标注等），应明确安全协议，包含保密条款、违约追责要求，建立服务商安全资质审核标准。

8 技术要求

平台数据安全技术的总体目标是保障平台数据的机密性、完整性和可用性。

本平台原则上不应承载核心数据与重要数据；如业务确需接入核心、重要数据，应制定专项安全管控方案。

平台内数据如涉及出境，应满足船旗国及主管机关法律法规要求。

平台全生命周期安全防护框架可采用 CCS GD016-2021 给出的船舶数据安全框架，见图 1。

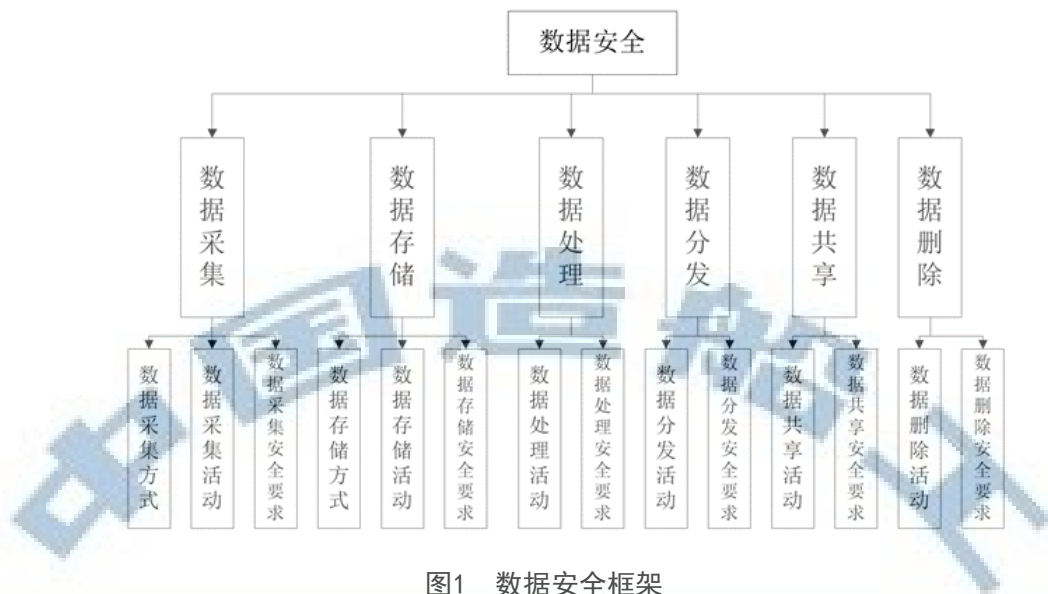


图1 数据安全框架

8.1 数据采集安全要求

平台开展数据采集活动应满足下列安全要求：

- a) 定义采集数据的目的和用途，明确数据采集源、采集数据类型和采集数据范围；
- b) 遵循合规原则，确保数据采集的合法性、正当性和必要性；
- c) 遵循最小化原则，只采集满足业务所需的最少数据；
- d) 遵循质量保障原则，制定数据质量保障的策略、规程和要求；
- e) 遵循确保安全原则，对采集的数据进行分类分级标识，并对不同类和级别的数据实施相应的安全管理策略和保障措施。对数据采集环境、设施和技术采取必要的安全管控措施。

8.2 数据存储安全要求

平台开展数据存储活动应满足下列安全要求：

- a) 对不同类别、不同级别的数据实施隔离存储，可采用物理隔离或逻辑隔离机制；
- b) 落实存储安全管控，涵盖存储架构安全、逻辑存储安全、存储访问控制、副本安全、归档安全、数据时效性管理；
- c) 建立存储冗余策略、数据备份与恢复管理制度，规范备份恢复操作流程。

8.3 数据处理安全要求

平台开展数据处理活动应满足下列安全要求，分布式节点、数据分析、加密、脱敏等实现可参照 GB/T 35274-2023 相关条款：

- a) 依据个人信息、重要数据保护相关法规，明确数据处理目的与范围；
- b) 建立数据处理内部责任制度，保证数据分析和使用不超出声明的使用目的和范围；
- c) 遵循最小授权原则，提供细粒度的数据访问控制机制；
- d) 落实处理环节安全管控，包含分布式处理安全、数据分析安全、数据加密、敏感数据脱敏、全流程数据溯源；
- e) 遵循可审计原则，完整记录数据处理过程中的各类操作；
- f) 对数据处理输出结果开展风险评估，避免输出结果中包含可复原的敏感数据。

8.4 数据分发安全要求

平台开展数据分发活动应满足下列安全要求：

- a) 遵循责任不随数据转移原则；
- b) 在数据分发前，对数据进行风险评估，确保数据分发后的风险可承受，并通过合同明确数据接收方的数据保护责任；

- c) 在数据分发前,对数据的敏感性进行评估,根据评估结果对需要分发的敏感信息进行脱敏操作;
- d) 遵循可审计原则,记录时间、分发数据、数据接收方等相关信息;
- e) 评估数据分发中的传输安全风险,确保数据传输安全;
- f) 提供有效的数据安全共享机制;
- g) 建立数据发布的审核制度,明确数据发布的内容和范围对发布的数据开展定期审核。

8.5 数据共享安全要求

平台进行数据共享可依托统一数据分发机制,结合安全技术措施管控共享行为,防范窃取、泄露风险。统一分发机制应覆盖全部共享业务场景,例如原始分析结果向第三方共享、分析报告下载至办公终端等,对不同场景设置差异化安全控制流程。

平台开展数据共享活动应满足下列安全要求:

- a) 共享前完成数据分级、敏感性评估;
- b) 通过协议明确共享双方安全责任边界;
- c) 记录共享操作审计日志;
- d) 对共享输出的数据开展脱敏、去标识化处理。

8.6 数据删除安全要求

平台开展数据删除活动应满足下列安全要求:

- a) 对超过留存期限的数据执行删除,法律法规对留存期限有明确规定的遵从其规定;
- b) 根据数据分类分级建立对应删除销毁机制,明确销毁对象、销毁方式与操作流程;
- c) 遵循可审计原则,建立数据删除管理制度,记录删除操作时间、操作人员、操作方式、数据对象等审计信息。