ICS 35.020.05
CCS L 05

T/CICC

中 国 指 挥 与 控 制 学 会 团 体 标 准

T/ CICC 35020—2025

复杂智能系统维护性技术要求

Technical requirements for maintainability of complex intelligent systems

2025-11-20 发布　　2025-11-20 实施

中国指挥与控制学会　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。

本文件由中国指挥与控制学会提出并归口。

本文件起草参与单位：北京航空航天大学、杭州市北京航空航天大学国际创新研究院（北京航空航天大学国际创新学院）、中国航空工业集团公司沈阳飞机设计研究所、中国科学院声学研究所、中国电子科技集团公司信息科学研究院、潍柴动力股份有限公司、可靠性与环境工程技术国家级重点实验室、北京航空航天大学可靠性工程研究所、北京科技大学、武汉多谱多勒科技有限公司。

本文件主要起草人：杨顺昆、张昱昊、王永来，刘东、郝程鹏、徐珞、窦全礼、司昌龙、吴梦丹、翟长辉、林焱辉、杨乐昌、姚琪、孙国强、张永、王竞争、王天琪、周喆平。

复杂智能系统维护性技术要求

1 范围

本文件规定了复杂智能系统维护性的核心对象、定量与定性要求及支撑技术方法，并针对不同模型架构与功能类型，细化了对应的维护性要求。

本文件适用于复杂智能系统在需求、设计、训练、测试、运行、维护与退役阶段的各项维护性活动。

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。

GJB 451A-2005	可靠性维修性保障性术语
GB/T 11457－2006	信息技术 软件工程术语
GB/T 40571-2021	智能服务 预测性维护 通用要求
GJB 2072-94	维修性试验与评定
GB/T 41867— 2022	信息技术 人工智能 术语
GB/T 42018-2022	信息技术 人工智能 平台计算资源规范
GJB 3872A-2022	装备综合保障通用要求
GB/T 44407-2024	智能服务 预测性维护 虚拟维护系统技术要求
GB/T 45958—2025	网络安全技术 人工智能计算平台安全框架
T/CICC 35012－2025	复杂智能系统可靠性技术要求

3 术语与定义

GB/T 41867—2022、GB/T 45958—2025、GB/T 42018—2022 确立的以及下列术语和定义适用于本文件。

3.1

复杂智能系统 complex intelligent systems

由感知、认知、决策与执行等功能模块构成，采用机器学习等方法，在不确定、开放环境下执行任务的人机环管协同系统。其复杂性体现在多源异构数据、动态场景、要素耦合以及全生命周期演化。

[来源：T/CICC 35012－2025，9.12]

3.2

维护性 maintainability

指产品或系统能够被有效和高效地修改，以改进功能、修正缺陷或使其适应环境和需求变化的能力。

3.3

智能系统维护性　　intelligent system maintainability

指智能系统在全生命周期内，针对其数据、模型、算法、平台、知识及任务等核心对象，能够通过智能化手段（如自监测、自诊断、自修复与自演化）实现高效、安全、可追溯的维护与优化能力。

3.4

AI平台　　platform for AI

为 AI 应用提供计算、存储、网络与开发运维能力的软硬件与服务集成，包括但不限于 CPU、GPU、AI 加速器、系统软件、中间件、框架与接口等。

[来源：GB/T 45958—2025，3.1，有修改]

3.5

运行稳定性　　operation stability

指系统在连续运行过程中，性能指标（如吞吐、时延、误差）随时间的波动保持在设计容差内的特性。

3.6

模型退化　　model degradation

在给定任务与评估口径下，模型性能因时间、数据分布、硬件/软件环境变化而出现系统性下降的现象。

3.7

训练　　training

在给定的训练数据及约束条件下，通过优化算法调整模型参数以最小化（或最大化）预定目标函数的过程。

[来源：GB/T 42018—2022，3.11，有修改]

3.8

推理　　inference

在模型参数固定的情况下，模型对给定输入生成输出结果（如预测、分类、决策或评分）的过程。

注：推理通常在部署与运行阶段进行，与训练阶段的参数更新相区分，可包含不确定性估计与置信度输出。

[来源：GB/T 42018—2022，3.12，有修改]

3.9

训练集　　training set

用于估计和更新模型参数的数据集。

注：训练集应与验证集、测试集在样本层面互不重叠；对时间序列或主体相关数据，应采取时间/主体隔离以防信息泄漏。

[来源：GB/T 41867—2022，3.2.34，有修改]

3.10

测试集　　test set

用于在模型训练与选择完成后，对模型在未见数据上的性能进行客观评估的独立数据集。

注：测试集仅用于最终评估，不应用于任何形式的训练或调参决策。

[来源：GB/T 41867—2022，3.2.3，有修改]

3.11

验证集　　validation set

用于模型开发阶段选择模型结构、调参与早停等的独立数据集，不参与模型参数的最终训练。

注：验证集应与训练集、测试集互不重叠，避免信息泄漏。

[来源：GB/T 41867—2022，3.2.35，有修改]

3.12

数据漂移　　data drift

数据分布随时间或场景变化而发生的统计性质改变，导致训练异常。

[来源：ISO/IEC 5259—1 术语框架，有修改]

3.13

泛化能力　　generalization ability

模型在与训练数据分布相同或相近的未见样本上保持预期性能

注：可通过测试集性能、交叉验证、分布外评估等方式间接衡量。

3.14

鲁棒性　　robustness

在扰动、噪声或分布偏移条件下维持功能/性能的能力。

[来源：GB/T 41867—2022 3.4.9 有修改]

3.15

分布外　　out-of-distribution

偏离训练数据分布的输入样本或场景

3.16

模型修复　　model repair

指针对已部署神经网络模型出现的性能下降、偏移或功能错误等问题，通过不完全重训的方式（如精调、打补丁、结构重构）进行局部修复，使其恢复或优化原有性能的过程。

3.17

模型补丁　　model patching

指利用外部逻辑模块或输入控制策略对 AI 模型的特定错误区域进行校正，而无需修改原始模型参数。该技术适用于“黑盒模型”，并与可解释性分析紧密结合。

3.18

模型精调　　model fine-tuning

指在预训练模型基础上，以少量任务相关数据对特定参数进行微调优化的过程。其目标在于快速适应新场景或修复任务漂移带来的性能下降。常见方式包括 LoRA、Adapter、Prefix Tuning 等轻量化策略。

3.19

对抗性鲁棒修复　　adversarial robustness recovery

针对模型面临对抗样本攻击或极端输入扰动时产生的非预期行为，采用特定策略（如对抗训练、输入防御机制）增强模型鲁棒性的过程。

3.20

后训练　　post training

是指在模型的预训练阶段完成后，为进一步提升其在特定任务或场景下的性能与安全性，所进行的一系列附加训练或微调步骤。

4 缩略语

下列缩略语适用于本文件：

OOD	分布外 (Out-of-Distribution)
CI/CD	持续集成/持续部署 (Continuous Integration / Continuous Deployment)
MTTR	平均修复时间 (Mean Time To Repair)
DNN	深度神经网络 (Deep Neutral Network)
LLM	大语言模型 (Large Language Model)
RL	强化学习（Reinforcement Learning）
FT	模型精调（Fine-Tuning）

5 复杂智能系统维护性核心对象

5.1 数据对象

5.1.1 范围与构成

数据对象是指支撑智能系统开发、验证与运行的各类数据集合，通常包括：

a）训练数据与衍生数据；
b）验证数据与基准数据集；
c）运行时采集数据；
d）修复与维护数据集；
e）元数据与数据谱系；
f）对抗与异常数据。

5.1.2 边界与接口

数据对象的边界包括：

a）数据来源；
b）采集条件；
c）预处理与增强策略；
d）分割与抽样策略；
e）版本与追溯标识；
f）访问与控制策略。

数据对象与模型对象的接口包括：

a）特征与标签规范；
b）数据模式与输入分布；
c）数据质量指标与约束；

数据对象与系统对象的接口包括：

a）数据存储与传输协议；
b）带宽与时延约束；
c）缓存与容错策略。

数据对象与算法对象的接口包括：

a）数据预处理与特征映射规则；
b）算法输入输出协议与张量结构；

c）数据漂移与性能监测机制。

数据对象与知识任务对象的接口包括：

a）数据到知识的映射与抽取规则；

b）知识一致性与追溯接口；

c）知识更新与验证机制。

5.2 模型对象

5.2.1 范围与构成

模型对象是智能系统的核心组件，涵盖从传统机器学习到大规模深度学习模型，通常包括：

a）模型架构；

b）参数与权重；

c）超参数；

d）训练快照与检查点；

e）校准与不确定性估计模块；

f）对抗防御与鲁棒性增强模块。

5.2.2 边界与接口

模型对象的边界与接口包括：

a）输入/输出张量规范；

b）模型版本与回滚机制；

c）模块化替换插件；

d）热更新与持续学习接口；

e）模型验证和诊断工具链；

f）模型部署形态（云/边/端）。

5.3 算法对象

5.3.1 范围与构成

算法对象是支撑智能系统核心功能实现的逻辑与规则集合，通常包括：

a）数据处理与特征提取算法；

b）模型训练与优化算法（如梯度下降、遗传算法等）；

c）推理与决策算法（包括搜索、规划、推理引擎）；

d）强化学习与自适应控制策略；

e）算法加速与近似计算方法；

f）算法安全与防御机制（对抗样本检测、鲁棒性增强等）。

5.3.2 边界与接口

算法对象的边界与接口包括：

a）输入/输出格式与数据流；

b）算法复杂度与资源消耗边界；

c）参数调度与优化接口；

d）与硬件对象的加速适配接口；

e）算法测试与验证工具链。

5.4 AI平台对象

5.4.1 范围与构成

AI平台对象是支撑复杂智能系统数据、模型、算法及任务全生命周期运行与维护的智能化基础环境，其功能不仅限于计算与存储资源调度，更强调系统级的可监测性、可诊断性、可修复性与可演化性。通常包括：

a）基础支撑层：提供计算、存储、网络及异构硬件资源，支持云-边-端协同运行与维护；

b）智能调度与编排层：具备任务调度、资源预测与弹性伸缩能力，支持多模型多任务的隔离、迁移与在线回滚； 模型服务与部署组件；

c）开发运维层：提供模型注册、版本管理、自动化训练与部署工具链，具备日志归档、指标监控及异常告警机制； 评测平台，用于在多场景、多指标下验证模型性能与安全性，支持基准评测、对抗测试、分布外检测及维护性指标的自动统计；

d）自诊断与修复层：具备运行状态感知与健康度评估功能，可基于异常检测、根因分析与预测性维护算法实现平台级自修复；

e）安全与合规层：保障平台在维护与更新过程中的访问控制、数据安全、可信执行与合规性；

f）演化与知识层：通过持续学习与经验积累实现维护知识沉淀、策略优化与自演化。

5.4.2 边界与接口

AI平台对象的边界与接口包括：

a）资源层接口：规定计算、存储与网络资源的分配与调度边界，支持多租户环境下的隔离与资源弹性恢复机制；同时应提供硬件配置查询、驱动更新与模块替换接口，支持硬件维护自动兼容验证；

b）软件与组件接口：提供软件上传、版本注册与模块替换API，支持在不中断服务的条件下进行软件包加载、依赖校验与组件回滚；

c）模型与算法层接口：提供模型注册、部署与推理API；支持多框架兼容与模型热更新； 模型注册与推理服务的API接口；

d）监测与诊断接口：定义性能指标采集、日志追溯与异常事件上报规范，支持跨节点的状态同步与故障定位； 平台与系统对象间的安全隔离与可信执行接口。

e）维护与修复接口：支持自动化维护任务的触发、执行与验证，包括在线修复、版本回滚、差分更新与健康度复检；

f）安全与可信接口：实现访问控制、身份认证、签名验证与安全审计；

g）演化与反馈接口：支持基于维护日志与运行数据的知识回流与策略优化，实现平台自学习与持续改进。

5.5 知识对象

5.5.1 范围与构成

知识对象是指系统中可更新、可维护的识结构与任务逻辑，通常包括：

a）知识图谱与规则库；

b）本体与语义模型；

c）价值对齐与伦理约束模块；

d）可解释性与因果关系表示模块。

5.5.2 边界与接口

知识对象的边界与接口包括：

a）知识抽取与更新接口；

b）规则热插拔接口；

c）决策可追溯性记录；

d）推理调用与反馈验证接口；

e）知识一致性与版本追溯接口。

5.6 任务对象

5.6.1 范围与构成

任务对象是智能系统执行目标与逻辑的核心定义单元，包含任务描述、状态转移与评估机制，通常包括：

a）任务目标与评价指标；

b）状态与动作空间定义；

c）任务分解与调度逻辑；

d）人机协作与交互策略。

5.6.2 边界与接口

任务对象的边界与接口包括：

a）与模型对象的输入输出映射接口；

b）与AI平台对象的任务调度与资源分配接口；

c）与知识对象的逻辑约束与依赖接口；
d）与系统对象的控制信号接口。

5.7 接口对象

5.7.1 范围与构成

接口对象是指支撑复杂智能系统各核心要素（数据、模型、算法、平台、知识、任务）之间交互、协同与信息流通的通信与协议集合。接口对象不仅包括传统意义上的API、通信协议和中间件适配层，还涵盖智能系统运行中的语义契约、消息语义、行为规范与反馈机制等，是维护性实现与验证的关键通道。

a）数据接口：实现数据采集、传输、存储与访问的统一规范，包括数据格式、传输协议、加密方式与访问控制；
b）模型接口：定义模型输入输出结构、推理调用方式及版本兼容机制； 任务分解与调度逻辑；
c）算法接口：约束算法模块之间的调用与参数传递规则，确保不同算法实现可插拔与可替换；
d）平台接口：实现资源管理、任务调度、日志采集与安全认证的通信通道；
e）知识接口：用于知识更新、规则验证与逻辑推理调用；
f）人机接口：为运维人员与系统交互提供图形化与命令化通道，支持可视化维护与解释性反馈；
g）外部接口：支持与外部系统、云服务、边缘节点或异构智能体的协同交互。

5.7.2 边界与接口

接口对象的边界应明确交互范围、权限与安全策略，并建立版本追溯与一致性验证机制。主要内容包括：

a） 接口定义边界：明确接口输入输出参数、调用频率、时延容差及数据类型约束；
b） 安全边界：通过身份认证、访问控制、加密与审计机制，防止接口越权调用与信息泄漏；
c） 兼容性边界：确保接口在不同版本、不同平台与不同部署模式下保持兼容；
d） 异常边界：当接口出现异常（如通信中断、参数错配、数据漂移）时，应具备回退、熔断与重试机制；
e） 验证接口：定义接口健康度检测、延迟监控与一致性校验机制，支持自动化测试与验证。

5.7.3 与其他对象的关系

接口对象贯穿复杂智能系统各层，与其他核心对象关系如下：

a）与数据对象：确保数据流通与治理过程的安全、可控、可追溯；
b）与模型对象：支撑模型输入输出标准化、跨版本兼容与热更新；
c）与算法对象：提供算法复用与模块化替换的通信机制；
d）与平台对象：连接资源调度、监控与自修复模块；
e）与知识对象：实现知识更新与推理验证的双向交互；
f）与任务对象：保障任务调度、执行与反馈过程的完整性与一致性。

6 复杂智能系统维护性定性要求

6.1 数据维护性要求

对数据维护性提出要求，包括数据版本追溯、数据修复一致性、数据冗余备份与漂移检测等，具体内容如下：

a）智能系统应具备数据版本管理能力，能够追溯至具体采集批次、标注版本及使用场景；
b）智能系统应在数据修复后进行一致性验证，保证修复数据与基准数据集在关键指标上一致；
c）智能系统应配置数据冗余与备份机制，确保在存储或传输异常情况下可快速恢复
d）智能系统应具备数据漂移监测能力，在分布显著变化时发出维护警告。

6.2 模型维护性要求

对模型维护性提出要求，包括模型版本管理与回滚、模型更新方式、模块化修复与修复验证等，具体内容如下：

a）智能系统应具备模型版本管理与回滚机制，确保新模型性能不达标时可恢复到上一稳定版；
b）智能系统应支持模型热更新或平滑切换，避免维护过程中服务中断；
c）智能系统应具备模块化修复能力，在模型局部失效时能替换单一模块而非整体重构；

d）智能系统应提供模型修复验证机制，包括自动化测试用例与基准数据集，用于验证修复后的性能与安全性。

6.3 平台维护性要求

对平台维护性提出要求，包括硬件与操作系统更新后的兼容性、回滚与熔断机制、跨平台维护支持与平台健康监测等，具体内容如下：

a）智能系统应在硬件平台或操作系统更新后，保证关键功能的兼容性与稳定性；

b）智能系统应具备回滚与熔断机制，当平台更新失败或引发异常时，能够恢复至安全状态；

c）智能系统应具备跨平台维护支持，在不同计算环境（云、边、端）下保持一致的运行与修复策略；

d）智能系统应提供平台健康监测功能，对硬件故障、存储异常、网络延迟等情况进行预警。

e）智能系统应具备运行态自诊断与异常预测能力，能够基于性能指标与运行日志识别潜在退化趋势，并触发维护预警或自修复流程；

f）智能系统应具备安全与合规保障能力，在平台更新、修复与迁移过程中保持数据加密、访问控制和审计追溯的连续性；

g）智能系统应建立统一的维护知识与经验复用机制，在平台内形成维护案例库与策略优化模型，支持维护流程持续改进。

6.4 功能维护性要求

对功能维护性提出要求，包括核心功能连续性、功能级降级运行、接口版本兼容与替换机制等，具体内容如下：

a）智能系统应确保在维护操作（数据修复、模型更新、平台升级）过程中，核心功能的连续性不受影响；

b）智能系统应支持功能级降级运行，在部分模块异常时，系统能以降低性能或受限方式继续运行；

c）智能系统应提供功能接口的版本兼容机制，避免因接口变化造成功能失效；

d）智能系统应在关键功能失效时，具备快速替换或旁路机制，缩短恢复时间。

6.5 安全维护性要求

对安全维护性提出要求，包括维护过程中的访问控制、维护日志记录、安全校验与异常保护等，具体内容如下：

a）智能系统应在维护操作过程中，保证数据安全与访问控制，防止越权操作；

b）智能系统应对维护日志进行完整记录，确保维护行为可追溯、可审计；

c）智能系统具备安全校验机制，在更新数据、模型或平台组件时进行签名验证与完整性校验；

d）智能系统应在维护操作失败或异常情况下，自动进入安全态或受限态，避免扩散性故障。

6.6 知识维护性要求

对知识维护性提出要求，包括知识更新、一致性校验、可追溯性及人机协同维护等方面，具体内容如下：

a）智能系统应具备知识版本管理与追溯机制，确保不同版本的规则与事实可比对、可回滚；

b）智能系统应支持知识库的增量更新与动态扩展，保证在逻辑一致性与依赖完整性条件下完成知识扩充；

c）智能系统应在知识更新后自动执行一致性检查，防止逻辑冲突、冗余或推理错误；

d）智能系统应提供知识验证与修复工具，用于识别和更正失效或偏差知识条目；

e）智能系统应建立人工审核与反馈机制，实现知识更新过程中的人机协同；

f）智能系统应对知识修改过程进行完整记录与审计，确保可追溯与可验证。

6.7 任务维护性要求

对任务维护性提出要求，包括任务定义、调度、验证与安全回退，具体内容如下：

a）智能系统应具备任务模板与配置的版本管理机制，支持任务定义的可复现与对比；

b）智能系统应支持任务逻辑的动态调整与在线更新，适应运行环境与模型变化；

c）智能系统应建立任务执行验证机制，对结果一致性与性能进行自动检测；

d）智能系统应具备任务回滚与重试机制，保障在执行异常时快速恢复；

e）智能系统应记录任务全生命周期信息，用于后续维护与风险分析。

7 复杂智能系统维护性定量指标

智能系统维护性指标及计算方法如表1所示：

表 1 智能系统维护性定量要求

序号	指标	含义	计算方法	备注
1.	平均模型热更新时间	在不中断服务的前提下完成一次参数更新或增量部署的平均耗时。	$MMTU = \frac{\sum T_{update}}{N_{update}}$ MMTU: 平均模型热更新时间； $\sum T_{update}$ ：所有热更新任务的耗时总和； N_{update} ：热更新任务的次数。	数值越小越好，用于在线更新。
2.	平均修复时间	系统或设备在发生故障后，完成修复并恢复正常运行所需时间的平均值	$MTTR = \frac{T}{N}$ MTTR: 平均修复时间； T: 所有故障发生后到恢复运行耗时总和； N: 故障发生的次数；	衡量 维护效率的关键指标。
3.	微调收敛时间	在指定数据集上完成一次增量微调并达到预定性能阈值的平均迭代次数或时间。	记录达到性能阈值（如准确率≥X）的最短迭代步数/时间。	衡量大模型维护的效率。
4.	模型漂移检测延迟	从数据分布发生显著漂移到系统检测出漂移的时间间隔。	$L_{drift} = T_{detect} - T_{occur}$ L_{drift} ：模型漂移检测延迟； T_{detect}：系统检测出漂移的时刻； T_{occur}：从数据分布显着漂移到的时刻。	越短越好，体现对运行环境的适应能力。
5.	对抗修复成功率	在遭受对抗样本攻击后，通过修复（防御模块/再训练）恢复性能的比例。	$R_{adv} = \frac{N_{succ}}{N_{attack}}$ R_{adv} ：对抗修复成功率； N_{succ} ：修复（如防御/再训练）后恢复性能的成功次数； N_{attack} ：遭受对抗攻击的总次数。	针对深度学习的安全维护性。
6.	模型参数回滚成功率	在新版本模型更新失败时，成功恢复到前一版本并稳定运行的比例。	$R_{rollback} = \frac{N_{succ}}{N_{attack}}$ $R_{rollback}$ ：模型参数回滚成功率； N_{succ} ：在新版本模型更新失败时，成功恢复到前一版本的次数； N_{attack} ：尝试模型更新的总次数。	体现模型的安全回退机制。
7.	模块化替换时间	在不影响整体运行的情况下，替换单一模块（如注意力头/适配器）的平均耗时。	$T_{replace} = \frac{\sum T_i}{N}$ $T_{replace}$ ：替换单个模块（如注意力头/适配器）的平均耗时； ∑Ti ：所有模块替换任务的耗时总和； N: 模块替换任务的总次数。	数值越小越好，适于参数高维的模型。

8 复杂智能系统维护性支撑技术与方法

8.1 复杂智能系统运行观测与数据治理

8.1.1 运行观测体系

8.1.1.1 运行数据采集

应在系统运行时建立全方位数据采集机制，其内容包括：

a）运行日志、调用链及事件序列的完整采集；

b）传感器数据（CPU、内存、I/O、带宽等）实时监控；
c）模型内部状态参数（置信度、特征向量、梯度等）的采样；
d）运行时异常事件的时间戳与上下文记录；
e）用户交互与输入数据的统计分布监控；
f）关键性能指标（延迟、吞吐量、错误率）的持续采集。

8.1.1.2 数据规范与治理

应建立统一的数据治理规范，其内容包括：
a）运行数据的清洗、去噪与标准化处理；
b）数据漂移检测与分布一致性验证；
c）元数据（版本、时间、来源）的自动化管理；
d）数据完整性校验与冗余存储策略；
e）跨系统的数据接口标准化；
f）安全与合规性要求（加密、访问控制、审计追踪）。

8.1.2 异常可视化与解释机制

8.1.2.1 异常结果可视化

应建立异常检测结果可视化机制，其内容包括：
a）关键运行指标（延迟、精度、吞吐量）的实时趋势图；
b）输入数据分布与模型输出分布的对比展示；
c）异常事件链路可视化（调用依赖、模块关联）；
d）异常严重程度和影响范围的图形化标注；
e）支持交互式放大、筛选和过滤的可视化工具。

8.1.2.2 可解释性分析

应采用解释性方法分析系统异常，其内容包括：
a）采用局部可解释模型；
b）特征重要性与贡献度热力图；
c）因果图谱驱动的异常因果分析；
d）决策路径追溯与特征权重可视化；
e）交互式异常溯源工具，支持人工与自动结合分析。

8.2 复杂智能系统缺陷预测与智能诊断

8.2.1 缺陷预测方法

8.2.1.1 退化与寿命预测

应建立退化建模与寿命预测方法，其内容包括：
a）基于统计建模与时间序列分析的剩余使用寿命估计；
b）性能退化曲线拟合与阈值预测；
c）基于状态空间模型的健康度评分；
d）多维特征融合的退化趋势外推；
e）结合历史案例库的寿命预测对比分析；
f）预测结果的置信区间与不确定性量化。

8.2.1.2 数据与模型缺陷预测

应建立多维度缺陷预测方法，其内容包括：
a）数据质量缺陷预测，包括缺失率、噪声水平与漂移趋势；
b）模型性能退化预测，包括精度下降率与过拟合风险；
c）输入输出异常分布的提前检测与偏移预测；
d）计算与存储资源消耗瓶颈的预测与预警；
e）预测性维护模型应用于异常趋势分析；
f）多模型对比与集成预测以提升准确性。

8.2.2 智能根因诊断机制

8.2.2.1 故障溯源

应提供跨层溯源能力，其内容包括：

a）基于调用链与日志的异常传播路径追踪；

b）因果图谱驱动的关键因子定位；

c）基于图神经网络的依赖关系分析；

d）跨模块故障影响链路识别；

e）历史故障案例的模式匹配与相似度分析；

f）诊断结果的可视化展示与交互式溯源。

8.2.2.2 智能异常检测

应采用智能化异常检测方法，其内容包括：

a）基于自监督学习的特征表示异常检测；

b）对比学习驱动的潜在分布偏移检测；

c）跨模态数据融合异常检测（文本、图像、传感器数据）；

d）基于概率模型与贝叶斯方法的不确定性检测；

e）多尺度特征检测，支持局部与全局异常识别；

f）结合强化学习的自适应异常检测策略。

8.3 复杂智能系统安全热更新与修复规划

8.3.1 在线更新机制

8.3.1.1 更新策略

应采用多样化的在线更新策略，其内容包括：

a）蓝绿部署，保障新旧版本并行运行并平滑切换；

b）金丝雀发布，通过小规模用户群体先行测试新版本；

c）影子测试，在不影响真实业务的情况下对新版本进行对比运行；

d）灰度发布，分阶段逐步扩展新版本的应用范围；

e）基于特征开关的功能动态启用与关闭；

f）多环境并行验证（开发、预生产、生产环境）。

8.3.1.2 一致性保障

应保障更新过程中数据与系统状态的一致性，其内容包括：

a）事务一致性与数据回滚机制；

b）断点续传与差分更新机制，减少更新失败风险；

c）多版本共存策略，支持版本间兼容与切换；

d）跨节点同步与一致性协议；

e）更新过程中的系统健康度监控与阈值告警；

f）关键模块的冗余与自动降级机制。

8.3.2 模型修复机制

8.3.2.1 微补丁修复

应采用高效、轻量的模型修复方法，其内容包括：

a）参数高效FT方法；

b）增量模块插入与热插拔技术；

c）基于知识蒸馏的小规模模型修复；

d）在线增量训练以修正模型偏差；

e）自动化补丁生成与快速加载；

f）修复过程对运行时延与资源消耗的控制。

8.3.2.2 修复验证

应在模型修复完成后进行多维度验证，其内容包括：

a）影子部署验证，确保修复版本与原版本并行运行测试；

b）性能基准对比，包括精度、延迟与资源消耗指标；

c）异常率与误检率的持续监控；

d）跨场景与跨任务的通用性测试；

e）修复过程的可追溯性与审计记录；
f）验证结果的量化评估与门控发布机制。

8.4 复杂智能系统恢复保障

8.4.1 容错与恢复性设计

8.4.1.1 容错设计要求

应在系统各层建立容错机制，其内容包括：
a）关键模块的冗余配置，确保任一组件故障时系统可由备用模块接管；
b）局部错误的自动隔离与熔断机制，防止异常扩散；
c）任务重试与回退策略，保障在计算或通信失败时自动重新执行；
d）主备切换与一致性协议，确保数据与控制状态在切换后保持正确；
e）多副本存储与数据校验机制，用于防止损坏与误删；
f）资源分配与任务执行的错误检测机制，用于在调度层面快速识别并恢复。

8.4.1.2 运行连续性保障

应确保系统在出现局部故障或外部干扰时仍能维持核心功能，其内容包括：
a）关键任务的优先执行与隔离保护；
b）非关键模块的自动降级或暂停运行策略；
c）跨节点负载转移与任务重新分配机制；
d）基于仲裁的主备切换机制；
e）高负载条件下的动态资源调度与限流控制。

8.4.2 自恢复与修复机制

8.4.2.1 自动恢复

应建立自动化故障恢复机制，其内容包括：
a）异常检测与告警触发机制；
b）故障隔离与节点自动重启；
c）基于控制器的修复任务自动执行；
d）利用检查点与快照的回放恢复；
e）基于健康度阈值的自适应恢复策略；
f）恢复过程对业务影响的最小化控制。

8.4.2.2 恢复验证

应开展恢复后的系统验证，其内容包括：
a）恢复后功能完整性检查；
b）性能指标（吞吐量、延迟、准确率）的回归验证；
c）关键模块的健康度检测；
d）恢复过程日志与追溯分析；
e）恢复效果的量化评估（如MTTR、可用性比率）；
f）恢复后系统的持续监控与风险复检。

8.5 智能系统维护性验证与持续改进

8.5.1 维护性验证机制

8.5.1.1 更新与修复验证

应对更新与修复后的系统进行全面验证，其内容包括：
a）影子流量回放验证，确保新版本在真实数据上表现一致；
b）回归测试，验证修复是否引入新的缺陷；
c）基于性能基准的对比测试，包括吞吐量、延迟和准确率；
d）关键指标（MTTR、可用性、可靠性）的量化评估；
e）跨模块与跨场景的兼容性测试；
f）异常率、误检率和告警准确率的监控与对比。

8.5.1.2 安全与合规验证

应对维护活动开展安全与合规验证，其内容包括：

a）数据安全检查，包括加密存储与传输完整性；
b）访问控制与权限分配符合安全策略；
c）日志与审计追溯机制是否完整有效；
d）合规性检测；
e）修复补丁的合法性与完整性校验；
f）外部依赖组件的安全性验证与漏洞检测。

8.5.2 持续改进机制

8.5.2.1 在线学习与优化

应建立面向运行环境的持续学习与优化机制，其内容包括：
a）在线再训练机制，支持在安全环境下对模型增量更新；
b）基于迁移学习的模型优化与跨域适应；
c）异常与缺陷数据的动态采样与反馈学习；
d）自动化特征选择与模型结构优化；
e）运行中策略（调度、容错）自适应调优；
f）优化效果的量化对比与持续评估。

8.5.2.2 知识沉淀与复用

应建立维护知识库和案例库，实现经验归档与复用，其内容包括：
a）维护案例的结构化存储与分类管理；
b）缺陷与修复过程的知识图谱构建；
c）运维手册与标准化流程的自动生成与更新；
d）基于经验库的自动化诊断与决策支持；
e）跨系统与跨领域的知识共享与迁移；
f）维护经验与优化措施的定期复盘与改进。

9 基于模型架构类型的智能系统维护性

9.1 基于大模型的智能系统维护性要求

9.1.1 模型维护性要求

对大模型维护性提出要求，具体内容如下：
a）大模型应具备参数微调、增量更模块化替换机制，避免整体重训练带来的高成本；
b）应支持热更新与回滚功能，保证在模型更新失败或性能下降时能够迅速恢复；
c）应在不同硬件环境下提供轻量化版本，以适应多样化的运行条件。

9.1.2 平台与数据维护性要求

对大模型平台与数据维护性提出要求，具体内容如下：
a）应具备跨平台部署的维护能力，在云、边、端环境中保持一致的运行性能；
b）应提供训练/推理日志与版本管理机制，确保维护过程可追溯；
c）应具备数据漂移检测与报警功能，保证大模型在长期运行中的性能稳定。

9.2 基于联邦学习的智能系统维护性要求

9.2.1 模型维护性要求

对联邦学习模型维护性提出要求，具体内容如下：
a）联邦学习系统应支持节点版本管理与同步机制，保证不同终端的模型版本一致性；
b）应在节点资源不足或更新失败时，具备部分节点降级与替换的维护措施；
c）应支持跨时区、跨网络条件下的异步更新机制。

9.2.2 平台与数据维护性要求

对联邦学习平台与数据维护性提出要求，具体内容如下:
a）应提供终端数据源的维护自检机制，确保训练数据质量与格式一致性；
b）应在通信失败或带宽不足时，具备参数缓存与重传机制；
c）应支持分布式日志归档与节点更新追溯。

9.3 基于深度神经网络的智能系统维护性要求

9.3.1 模型维护性要求

对深度神经网络模型维护性提出要求，具体内容如下：

a）深度神经网络应支持模块化修复，如替换单一层或子网络，而非整体重构；

b）应提供剪枝、量化、蒸馏等轻量化维护方法，以适应资源受限环境；

c）应具备对抗修复机制，提升模型在遭受攻击后的恢复能力。

9.3.2 平台与数据维护性要求

对深度神经网络平台与数据维护性提出要求，具体内容如下：

a）应支持在不同操作系统与容器环境下的兼容性验证；

b）应提供数据漂移检测与维护日志，确保输入分布变化下的持续性能；

c）应在训练中断时，具备快照保存与断点续训功能。

9.4 基于迁移学习的智能系统维护性要求

9.4.1 模型维护性要求

对迁移学习模型维护性提出要求，具体内容如下：

a）迁移学习模型应支持快速适应新任务或新场景的增量更新，避免全量再训练；

b）应具备任务切换与参数冻结机制，减少因任务漂移导致的性能下降；

c）应在跨域迁移时，提供小样本/零样本学习维护工具，降低维护成本。

9.4.2 平台与数据维护性要求

对迁移学习平台与数据维护性提出要求，具体内容如下：

a）应在不同数据分布与标签空间下保持可维护性；

b）应支持源任务与目标任务之间的数据与模型追溯；

c）应提供跨域迁移日志与版本对比机制，便于风险控制。

9.5 基于Transformer模型的智能系统维护性要求

9.5.1 模型维护性要求

对 Transformer 模型维护性提出要求，具体内容如下：

a）Transformer模型应支持多任务模块化替换（如注意力头、适配器）

b）应具备热插拔与并行更新机制，保证更新时不中断服务；

c）应在边缘设备上提供轻量化版本。

9.5.2 平台与数据维护性要求

对 Transformer 模型平台与数据维护性提出要求，具体内容如下：

a）应支持多框架实现的兼容性维护；

b）应在长序列任务中具备显存优化与分布式维护策略；

c）应提供版本对比工具，确保更新后的性能稳定性。

9.6 基于扩散模型的智能系统维护性要求

9.6.1 模型维护性要求

对扩散模型维护性提出要求，具体内容如下：

a）扩散模型应支持逐步更新策略，避免一次性大规模重训；

b）应具备采样加速与部分替换机制，降低维护时的计算开销；

c）应支持不同模态（图像、音频、视频）下的统一维护接口。

9.6.2 平台与数据维护性要求

对扩散模型平台与数据维护性提出要求，具体内容如下：

a）应提供跨模态的日志追溯与测试工具；

b）应具备大规模训练的断点续训与参数快照保存机制；

c）应在显存受限条件下，支持动态批次调整。

9.7 基于强化学习的智能系统维护性要求

9.7.1 模型维护性要求

对强化学习模型维护性提出要求，具体内容如下：

a）强化学习系统应支持策略回滚与替换，在新策略退化时快速恢复；

b）应具备环境参数变化下的策略再适应维护工具；

c）应支持对抗性验证与修复，防止策略在异常状态下失效。

9.7.2 平台与数据维护性要求

对强化学习平台与数据维护性提出要求，具体内容如下：

a）应支持不同仿真环境与真实环境接口的一致性维护；

b）应在高延迟反馈场景下提供日志与数据缓存；

c）应具备多策略版本管理与对比机制。

9.8 基于多智能体的智能系统维护性要求

9.8.1 模型维护性要求

对多智能体系统模型维护性提出要求，具体内容如下：

a）多智能体系统应支持角色与数量变化下的自适应维护策略；

b）应具备冗余与任务再分配机制，在个体失效时保持整体功能；

c）应提供协同更新机制，确保多智能体在更新后保持一致性。

9.8.2 平台与数据维护性要求

对多智能体系统平台与数据维护性提出要求，具体内容如下：

a）应支持不同硬件平台下的跨节点维护；

b）应提供分布式日志与同步工具，保证协同运行的可追溯性；

c）应在通信网络异常时，支持临时本地维护与恢复机制。

9.9 基于分布式的智能系统维护性要求

9.8.1 模型维护性要求

对分布式系统模型维护性提出要求，具体内容如下：

a）分布式模型应支持跨节点参数同步与一致性维护，防止因网络延迟或节点故障导致的模型偏移；

b）应提供模型分区与模块化更新机制，使得局部模型可独立修复或替换，而不影响整体训练；

c）应在节点间建立版本控制与回滚机制，确保新版本发布失败时能够恢复到稳定状态；

d）应支持分布式检查点与快照保存机制，以便在中断或故障后快速恢复；

e）应具备跨节点模型性能对比与一致性验证功能，保障训练与推理结果的可重现性；

f）在异构计算环境下，应具备自动适配与资源调度能力。

9.8.2 平台与数据维护性要求

对分布式系统平台与数据维护性提出要求，具体内容如下：

a）应支持分布式环境下的安全维护，包括节点认证、数据加密传输与访问控制。

b）平台应支持分布式任务调度与故障自动转移机制，确保任务不中断；

c）应建立数据分片与副本管理机制，保障跨节点数据完整性与一致性；

d）应支持断点续传与差分同步功能，减少维护过程中的通信成本；

e）应提供节点状态监控与日志追溯工具，用于定位与修复异常节点；

f）应在网络波动或部分节点失联时具备自恢复与数据补偿机制。

9.10 基于群体智能的智能系统维护性要求

9.8.1 模型维护性要求

对群体智能系统的模型维护性提出要求，具体内容如下：

a）群体智能系统应支持个体行为模型的独立维护与批量更新，防止单个体故障影响整体性能；

b）应具备全局参数与局部策略的分层管理机制，保证群体协同行为的可控性；

c）应支持群体成员间的策略同步与知识共享机制，确保行为一致性与目标收敛性；

d）应在个体策略退化或异常时自动触发替换或重新训练流程；

e）应提供群体层面的性能评估与个体差异化分析功能，用于识别与修复失效成员；

f）在复杂动态环境下，应支持自组织维护策略，使群体结构能根据任务需求自调整。

9.8.2 平台与数据维护性要求

对群体智能系统平台与数据维护性提出要求，具体内容如下：

a）平台应支持多主体并行运行与通信调度，保障消息传递的时序一致性；

b）应建立群体级与个体级的数据采集与追踪机制，用于维护决策依据的完整性；

c）应在通信异常或节点缺失时具备本地缓存与延迟同步功能，防止信息丢失；

d）应支持群体行为的可视化监控与异常预警，便于维护与干预；
e）应具备群体级日志记录与回放功能，支持对整体行为的回溯与再现；
f）应在群体规模变化时自动调整资源分配与任务映射，保证运行与维护效率。

10 基于功能类型的智能系统维护性要求

10.1 感知功能的智能系统维护性要求

10.1.1 典型使用场景

涵盖图像识别、语音处理以及传感器数据融合等应用领域。
a）图像识别与目标检测；
b）语音识别与声学处理；
c）传感器信号融合。

10.1.2 维护性要求

要求确保数据一致性与模型的灵活更新，减少噪声干扰，提升系统的感知能力。
a）应具备数据采集与标注的版本追溯机制，确保感知模型输入的一致性；
b）应支持模型权重的热更新与模块化替换，以适应传感器变化或输入分布漂移；
c）应提供自动化数据清洗与异常检测工具，用于减少感知输入中的噪声与缺陷。

10.1.3 风险控制措施

应建立应对传感器故障、模型更新及安全校验等风险的有效控制策略。
a）应对传感器失效或输入异常提供降级机制，如切换至多模态冗余通道；
b）应在感知模型更新过程中进行实时验证，确保更新不影响关键任务识别精度；
c）应建立感知数据的安全校验机制，防止数据注入攻击或对抗样本干扰。

10.2 认知功能的智能系统维护性要求

10.2.1 典型使用场景

涉及知识推理、自然语言理解及深度学习模型的语义解析。
a）知识图谱构建与推理；
b）大模型的自然语言理解与多模态认知；
c）深度学习模型的语义解析与特征抽取。

10.2.2 维护性要求

要求支持认知模型的动态更新与任务适配，确保版本兼容性和历史结果可复现。
a）应具备知识库的可扩展与热更新能力，支持规则与事实的动态维护；
b）应支持模型FT与增量学习，以适应语义空间或任务需求的变化；
c）应提供认知功能的版本兼容机制，确保历史任务结果在新版本下可复现与对比。

10.2.3 风险控制措施

应进行一致性检查与偏差检测，确保认知模块的输出质量，防止错误传播。
a）应在知识更新时进行一致性检查，防止逻辑冲突或推理错误；
b）应在大模型认知任务维护中加入偏差与幻觉检测机制；
c）应对认知模块的输出进行可信度评估，降低错误传播至后续模块的风险。

10.3 决策功能的智能系统维护性要求

10.3.1 典型使用场景

涵盖强化学习策略、任务分配及规则触发等领域。
a）强化学习模型的策略规划（无人驾驶、机器人控制）；
b）大模型的指令解析与任务分配；
c）专家系统的规则决策与条件触发。

10.3.2 维护性要求

要求具备灵活的回滚机制、模块替换能力及决策更新的可解释性工具。
a）应具备策略回滚与恢复机制，在新策略退化时可迅速切换至稳定版本；
b）应支持决策模块的参数化调整与模块化替换，降低系统重构成；。
c）应提供决策过程的可解释性维护工具，用于验证策略更新的合理性。

10.3.3 风险控制措施

应确保策略更新的仿真验证与决策模型间的协调，防止错误决策对系统产生负面影响。

a）应在策略更新前进行仿真验证，防止不稳定决策进入真实环境；

b）应在多模型决策系统中配置仲裁机制，避免不同决策模型冲突；

c）应建立紧急停止与人工干预机制，防止错误决策造成严重后果。

10.4 执行功能的智能系统维护性要求

10.4.1 典型使用场景

包括机器人控制、工业流程控制及边缘设备实时控制等。

a）机器人臂运动与操作任务执行；

b）自动驾驶车辆的加减速与转向控制；

c）工业生产线的机械臂、传送机构与执行部件控制；

d）具身智能系统的运动协调与动作规划。

10.4.2 维护性要求

执行功能的维护性要求包括模块化升级、参数调优与跨平台适配，具体内容如下：

a）应支持执行算法模块的独立升级与替换，避免整体停机；

b）应具备动作参数与控制逻辑的自动调优与诊断机制，提高维护效率；

c）应支持跨硬件平台与驱动环境的兼容性验证，确保不同执行设备的一致响应；

d）应在执行任务中断或异常后支持动作恢复机制，实现平滑继续执行；

e）应建立任务指令与执行反馈的版本追溯机制，确保执行逻辑的可重现与可验证；

10.4.3 风险控制措施

为确保执行过程安全可靠，应在系统设计与维护阶段制定风险防控策略，具体包括：

a）应在执行模块更新前进行仿真与安全验证，防止参数或指令异常导致错误动作；

b）应在执行异常或设备失效时自动触发安全态（如急停、限幅、断电保护）；

c）应提供多层次的异常检测与冗余控制机制，防止错误指令传播；

d）应建立执行过程日志追溯与复现机制，支持问题定位与维护决策；

11 智能系统维护性全生命周期过程及主要活动

11.1 需求阶段主要活动

在需求阶段，应明确智能系统的维护性目标与约束条件，为后续设计、实现和运行奠定基础。需求阶段的维护性关注点包括指标定义、风险识别与验收条件；

a）明确系统维护性目标及验收条件，覆盖可追溯性、可修复性、可更新性与安全性；

b）提出可量化的维护性评价指标及阈值，用于后续验证和改进；

c）识别潜在维护风险与关键约束，如资源限制、运行环境不确定性等；

d）形成维护性需求说明文件，作为设计输入。

11.2 设计阶段主要活动

在设计阶段，应通过架构设计和模块化方法增强系统的可维护性，确保数据、模型和知识库能够灵活替换与扩展。设计阶段的维护性关注点包括模块化、接口预留和轻量化方案；

a）建立面向维护的系统架构，支持模块替换与组件级更新；

b）在设计中引入监控与自诊断机制，以支持后续运行阶段的状态感知；

c）采用轻量化与解耦设计，减少更新时的依赖传播；

d）预留在线更新、版本回退及验证接口，保障后期维护的安全性与一致性。

11.3 训练阶段主要活动

在训练阶段，应关注训练过程的可重现性与中断后的恢复能力，并确保模型可支持增量和持续学习。训练阶段的维护性关注点包括快照保存、断点续训与参数追踪。

a）建立训练日志、参数快照与数据追溯机制，实现训练过程的可验证；

b）配置断点续训与自动恢复功能，降低训练中断的风险；

c）采用量化性能指标（如收敛时间、资源消耗率）监测训练效率；

d）引入模型验证与偏差检测机制，提前发现性能退化趋势。

11.4 测试阶段主要活动

在测试阶段，应验证系统的维护性设计是否满足预期，包括模型回滚、数据修复与接口兼容性等方面。测试阶段的维护性关注点包括故障注入、对抗验证和基准对比。

a）通过基准测试与自动化验证评估系统的可维护性性能；
b）采用异常注入与对抗验证方法，检验系统在异常情况下的修复与恢复能力；
c）开展数据修复一致性与模块替换验证，确保修复后的系统性能稳定；
d）建立维护性测试用例库，用于持续评估与版本间对比。

11.5 运行阶段主要活动

在运行阶段，应建立实时监控和告警机制，确保系统在发现退化或异常时能快速响应。运行阶段的维护性关注点包括自动化监控、告警与在线修复。

a）建立运行数据采集与分析机制，监控关键性能指标与异常趋势；
b）部署自动化告警与状态诊断模块，实现对潜在退化与故障的提前预警；
c）应用在线修复与动态更新策略，保证系统在运行中可平滑维护；
d）通过持续观测数据实现性能趋势评估与维护性量化监控。

11.6 维护与更新阶段主要活动

在维护与更新阶段，应确保数据、模型和知识库的更新可控、安全，并能够通过回滚与自动化工具提高效率。该阶段的关注点包括版本管理、批量维护和周期性评价。

a）实施版本管理与回滚控制，确保更新过程的可控性与可追溯性；
b）结合模型修复与数据更新机制，实现最小影响范围内的功能修正；
c）利用预测性维护与智能诊断方法，识别潜在故障并提前干预；
d）对维护过程开展验证与记录，形成可量化的维护绩效数据；
e）定期复盘维护活动，持续改进维护流程与工具。

11.7 退役阶段主要活动

在退役阶段，应妥善处理系统数据与模型，防止安全风险，并为系统迁移与过渡提供支持。退役阶段的关注点包括安全销毁、档案保存与知识迁移。

a）执行数据与模型的安全处置，防止敏感信息泄露；
b）保存系统运行与维护档案，包括版本、日志、修复记录等；
c）提供知识迁移与模型交接方案，支持后续系统的平滑过渡；
d）对退役过程进行完整性审查与风险评估，确保系统关闭的安全与合规性。