



# 团 体 标 准

T/CES XXX-XXXX

## 本体驱动的电网数字化系统构建平台功能 能导则

Guidelines for functions of ontology-driven power grid digital system  
construction platform

（征求意见稿）

XXXX-XX-XX 发布

XXXX-XX-XX 实施

中国电工技术学会 发布

目 次

目 次.....I

目 次.....I

前 言.....III

引 言.....IV

1 范围.....1

2 规范性引用文件.....1

3 术语和定义.....1

4 符号、代号和缩略语.....3

5 总体架构.....3

5.1 使用者层.....4

5.2 展示层.....4

5.3 服务层.....4

5.4 智能层.....4

5.5 数据层.....4

5.6 稳态与敏态边界.....4

6 本体模型要求.....4

6.1 模型构成.....5

6.2 电网业务特征要求.....5

6.3 模型生成顺序.....5

6.4 模型校验.....6

6.5 模型最小必备要素.....6

6.6 模型版本管理.....6

7 稳态研发功能要求.....6

7.1 需求导入.....6

7.2 需求文档生成.....6

7.3 本体建模.....6

7.4 场景预演.....6

7.5 代码与契约生成.....6

7.6 约束文档生成与打包.....7

7.7 模型基线冻结.....7

8 敏态研发功能要求.....7

8.1 服务注册 .....7

8.2 行为与接口绑定 .....7

8.3 原子工具生成 .....7

8.4 组合技能编排 .....7

8.5 智能体与智能助手构建 .....7

8.6 运行时执行 .....8

8.7 装配配置回滚 .....8

9 数据与接口要求 .....8

9.1 数据要求 .....8

9.2 接口要求 .....8

9.3 性能与测试评估要求 .....8

10 安全与可信要求 .....8

10.1 数据安全 .....8

10.2 可信要求 .....8

10.3 护栏 .....9

10.4 AI 安全 .....9

10.5 模型安全 .....9

10.6 内容安全 .....9

11 其它功能要求 .....9

11.1 需求脱敏 .....9

11.2 模型本地化部署 .....9

11.3 运行态监控与审计 .....9

11.4 知识库管理 .....9

附录 A （资料性） 本体模型示例 .....10

参 考 文 献 .....11

## 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》给出的规则起草。

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。

本文件由中国电工技术学会提出。

本文件由中国电工技术学会标准工作委员会能源智慧化专委会工作组归口。

本文件起草单位：国网信息通信产业集团有限公司研发中心、国网信息通信产业集团有限公司、北京国电通网络技术有限公司。

本文件主要起草人：冯东、王兴涛、孟洪民、诸葛雪迎、孟庆丰。

本文件为首次发布。

## 引 言

随着人工智能技术与软件工程的深度融合，面向电网数字化系统的 AI 原生研发范式正在深刻改变软件的研发方式。传统电网数字化系统研发过程依赖人工完成需求分析、数据建模、代码实现与系统集成等环节，存在需求与实现脱节、语义信息在传递过程中丢失、人工智能生成内容缺乏可靠约束等问题。

本体驱动方法通过构建业务领域的本体模型，将业务实体、行为、规则等语义以结构化、可机读的方式显式表达，使人工智能在理解业务语义的基础上进行确定性建模与运行时装配，实现从需求到代码再到智能体的全流程贯通。稳敏双态将研发过程划分为稳态（建模）与敏态（装配）两种状态，稳态强调确定性与可重复，敏态强调运行时依赖与智能编排，二者协同形成完整的研发闭环。

# 本体驱动的电网数字化系统构建平台功能导则

## 1 范围

本文件规定了本体驱动的电网数字化系统构建平台的功能要求，包括术语和定义、符号、代号和缩略语、平台总体架构、本体模型要求、稳态研发功能要求、敏态研发功能要求、数据与接口要求、安全与可信要求以及其它功能要求。

本文件适用于本体驱动的电网数字化系统构建平台的规划、设计、开发、集成、评估与应用，也可供采用本体驱动方法开展 AI 原生软件研发的机构参考。

本文件所描述的功能要求具有可裁剪性。不同规模、不同安全等级的电网数字化项目可根据实际需求对平台功能进行裁剪：小型项目可聚焦需求导入、本体建模与代码生成等稳态核心功能；中大型项目可扩展场景预演、敏态智能体装配与运行态审计等功能；涉密或高安全等级项目应强化数据隔离、安全审计与护栏策略。

## 2 规范性引用文件

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

GB/T 11457—2006 信息技术 软件工程术语

GB/T 25069—2022 信息安全技术 术语

GB/T 25000.10—2016 系统与软件工程 系统与软件质量要求和评价（SQuaRE）第10部分：系统与软件质量模型

GB/T 25000.51—2016 系统与软件工程 系统与软件质量要求和评价（SQuaRE）第51部分：就绪可用软件产品（RUSP）的质量要求和测试细则

GB/T 35273—2020 信息安全技术 个人信息安全规范

GB/T 41373—2022 信息安全技术 网络数据分类分级要求

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

GB/T 42131—2022 人工智能 知识图谱技术框架

GB/T 43582—2023 信息技术 人工智能 大模型训练与计算能力要求

## 3 术语和定义

下列术语和定义适用于本文件。

### 3.1

**本体** ontology

对特定领域内存在的实体、概念及其相互关系进行形式化、规范化描述的知识体系，用于表达业务的语义模型。

### 3.2

**本体模型** ontology model

以结构化、可机读形式描述业务对象、行为、规则、场景等语义信息的模型，通常采用人类可读且版本可控的描述语言组织。

### 3.3

#### 本体驱动 `ontology-driven`

以本体模型作为人工智能理解业务语义的唯一入口，使人工智能先理解业务实体的语义定义，再进行数据采集、推理与生成的方法。

### 3.4

#### 稳态研发 `stable-state development`

以建模为核心的确定性研发状态，将需求转化为本体模型、物理表、接口契约与约束文档。稳态研发在模型定义与契约生成阶段不依赖真实服务运行，但生成的接口契约用于后续真实服务对接，具备确定性、可重复的特性。

### 3.5

#### 敏态研发 `agile-state development`

以装配为核心的运行时研发状态，将本体模型装配为可运行的智能体与智能助手。敏态研发相比传统配置化开发具有运行时按需编排、低代码装配、人工智能自主决策与持续演进的差异化优势，依赖运行时环境与人工智能编排。

### 3.6

#### 稳敏双态 `stable-agile dual-state`

将软件研发过程划分为稳态（建模）与敏态（装配）两种状态并协同运转的研发模式。

### 3.7

#### 原子工具 `atomic tool`

单个行为与单个接口一对一封装形成的、可被智能体调用的最小执行单元。在电网数字化场景下，原子工具宜按业务行为、服务接口或数据实体单一维度进行划分，避免跨多个业务域的粗粒度封装或过度细碎的单字段操作。

### 3.8

#### 组合技能 `composite skill`

由多个原子工具通过编排形成的、面向特定任务的多步骤执行能力。

### 3.9

#### 智能体 `agent`

基于运行时内核，能够自主理解目标、规划并调用工具完成任务的人工智能程序，主要面向开发者与构建者。

### 3.10

#### 智能助手 `assistant`

与智能体共用同一运行时内核、面向业务用户的对话式人工智能应用，偏重领域知识问答与引导。

### 3.11

约束文档 harness document

约束大语言模型在既定模型边界内生成业务逻辑、推理结果与代码的文档集合，用于禁止其脱离模型虚构。

### 3.12

护栏 guardrail

对智能体写操作进行安全约束的机制，包括幂等去重、权限校验与失败补偿等。

## 4 符号、代号和缩略语

下列符号、代号和缩略语适用于本文件。

AI：人工智能（Artificial Intelligence）

LLM：大语言模型（Large Language Model）

DDL：数据定义语言（Data Definition Language）

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

JSON：JavaScript 对象表示法（JavaScript Object Notation）

REST：表述性状态传递（Representational State Transfer）

ReAct：推理-行动-观察（Reasoning-Acting-Observing）

SSE：服务器发送事件（Server-Sent Events）

SQL：结构化查询语言（Structured Query Language）

YAML：YAML ain't markup language（YAML Ain't Markup Language）

## 5 总体架构

平台采用分层架构，自顶向下包括使用者层、展示层、服务层（稳态服务与敏态服务）、智能层与数据层。平台总体架构见图 1。

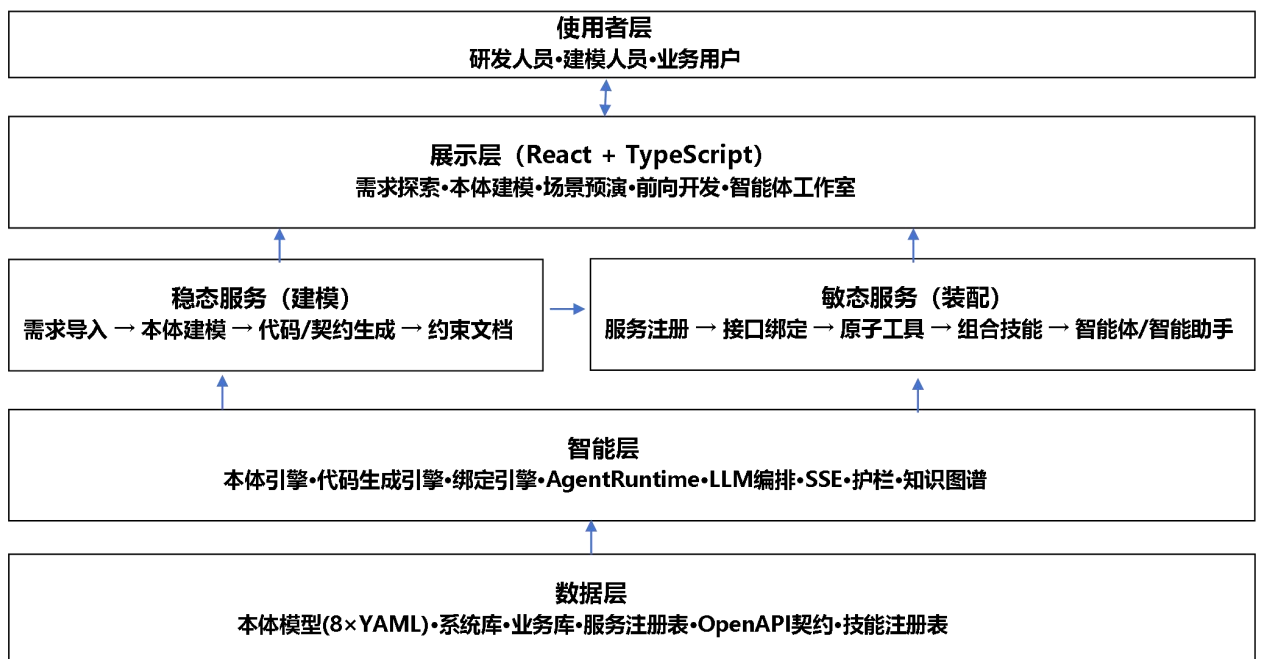


图 1 本体驱动的稳敏双态研发平台总体架构

## 5.1 使用者层

使用者层面向平台的不同用户角色提供差异化入口，包括业务人员、需求分析师、本体建模人员、开发构建人员、运维审计人员等。平台应支持按角色配置功能视图、权限范围与操作审批流程，确保各类使用者在统一平台上协同工作。

## 5.2 展示层

展示层为研发人员、建模人员与业务用户提供人机交互界面，应提供需求探索、本体建模、场景预演、代码与契约生成、接口映射、智能体工作室等功能入口，并以知识图谱、图表、流程图等形式直观呈现本体模型与研发过程。

## 5.3 服务层

服务层划分为稳态服务与敏态服务两类：稳态服务支撑需求导入、本体建模、代码与契约生成、约束文档生成等确定性建模过程；敏态服务支撑服务注册、接口绑定、原子工具生成、组合技能编排、智能体与智能助手构建等运行时装配过程。

## 5.4 智能层

智能层提供本体引擎、代码生成引擎、绑定引擎与智能体运行时等核心能力，负责大语言模型编排、流式输出、模型自修复、护栏校验与知识图谱构建。

## 5.5 数据层

数据层存储本体模型、系统数据库、项目业务数据库、服务注册表、接口契约以及技能与工具注册信息。

## 5.6 稳态与敏态边界

平台应明确稳态服务与敏态服务之间的边界接口：稳态产物（本体模型、接口契约、约束文档等）应经统一的模型仓库与注册接口向敏态侧发布；敏态侧应仅通过注册接口获取稳态产物，不应反向修改已冻结的稳态模型；稳态与敏态之间的交互应采用统一的认证、授权与审计机制。

平台应支持本体模型及平台组件的本地化部署，支持在内网或离线环境中运行，并支持接入本地部署的大语言模型服务。

# 6 本体模型要求

平台应以本体模型为核心驱动要素，采用八模型体系描述业务领域语义。八模型及其依赖关系见图 2。

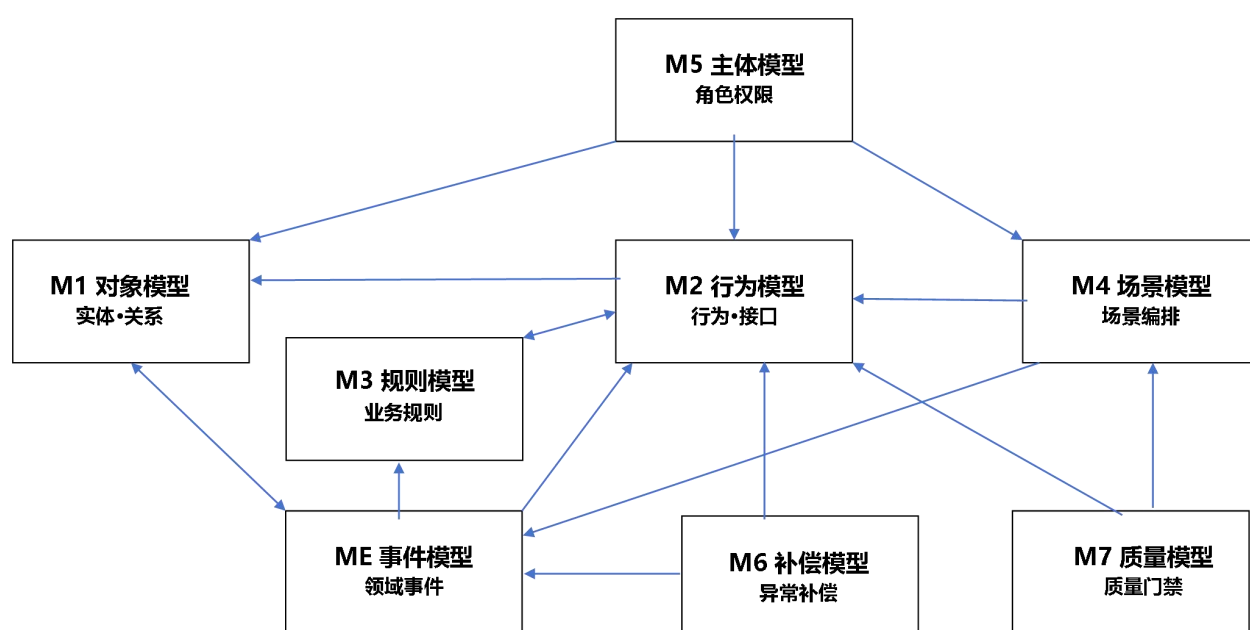


图 2 八模型本体体系及依赖关系

### 6.1 模型构成

八模型体系由下列模型构成，各模型应使用人类可读、版本可控的描述语言组织。推荐采用 YAML 或 JSON 格式进行描述，便于版本管理、差异比对与自动化解析；在跨厂商互操作时，宜优先采用 YAML 格式。

- M1 对象模型，定义业务实体、属性、关系与约束；
- M2 行为模型，定义分析与业务行为，标注计算类型与服务绑定；
- M3 规则模型，定义指标口径、业务规则与数据质量规则；
- M4 场景模型，定义分析场景编排与执行步骤；
- M5 主体模型，定义角色与权限；
- M6 补偿模型，定义异常补偿策略与回滚链；
- M7 质量模型，定义质量门禁与度量项；
- ME 事件模型，定义领域事件及其订阅与发布。

### 6.2 电网业务特征要求

本体模型应兼容电网业务特点，与通用领域模型相继承，宜满足下列要求：

- 以电网设备与资产（如变电站、输电线路、配电台区、电力用户等）为核心建模对象，支持电网统一对象分类与编码体系的对接；
- 支持电网拓扑关系建模，包括电气连接、空间隶属、量测关联等关系类型；
- 支持电网业务运行特征建模，包括运行方式、检修状态、业务时序与统计口径等；
- 支持电网典型业务场景（如调度运行、设备运维、营销服务等）的主体、权限与事件建模。

### 6.3 模型生成顺序

本体模型的生成应遵循依赖关系确定的顺序，宜按 M1 对象模型、M3 规则模型、M2 行为模型、M5 主体模型、M4 场景模型的顺序生成，M6、M7、ME 模型按需生成。在部分电网业务需求已先明确行为口径再补全对象属性的场景下，生成顺序可依据实际需求灵活调整，但应在平台中记录调整后的依赖关系与版本信息。

6.4 模型校验

每个模型生成后应经过结构校验，校验失败时应携带错误信息交由大语言模型自修复，自修复次数应予以限定（宜不超过 2 次），校验通过后方可落盘与持久化。若自修复次数达到上限仍无法通过校验，平台应抛出异常、终止当前生成流程并提示人工介入处理，同时保留错误日志与中间产物以供排查。

6.5 模型最小必备要素

八模型体系中的每个模型应至少包含下列最小必备要素：模型标识、模型名称、模型描述、版本号、依赖关系与责任主体。模型校验应检查最小必备要素的完整性与合法性，缺少最小必备要素的模型不得落盘与持久化。

6.6 模型版本管理

平台应对本体模型实行版本管理，模型的每次变更应生成新版本，并记录变更内容、变更人、变更时间与影响范围。模型版本应支持差异比对、历史追溯与回滚；模型形成稳定版本后，宜按 7.7 的规定进行基线冻结。

7 稳态研发功能要求

稳态研发功能实现从需求到模型的确定性转化，其流程见图 3。



图 3 稳态研发流程

7.1 需求导入

平台应支持导入原始业务需求文档，支持数据库模式与需求文档的上传，并具备对导入内容进行结构化解析的能力。平台应对导入的需求文档进行敏感信息识别与脱敏处理，脱敏规则应可配置，脱敏结果应可追溯。

7.2 需求文档生成

平台应依据需求模板，将原始需求解析为结构化的需求文档或需求规格文档。

7.3 本体建模

平台应依据需求文档按第 6 章规定的模型构成与顺序生成八模型，生成过程宜采用流式方式呈现，并构建反映实体关系的知识图谱。

7.4 场景预演

平台宜提供场景预演（校验）能力，在正式生成前对本体模型的场景链路进行模拟预演，用于校验模型的完整性与一致性。场景预演为可选环节，校验维度应至少包括：场景步骤完整性、行为与规则一致性、输入输出可达性、异常分支覆盖性。预演完成后应输出校验报告，报告宜包含：预演场景清单、通过的校验项、失败的校验项及原因、异常链路说明与修复建议。

7.5 代码与契约生成

平台应基于本体模型生成物理表 DDL、数据库表映射、数据服务与行为类代码、OpenAPI 接口契约以及规则函数代码等产物。生成的代码与 DDL 宜适配电网行业主流技术栈，包括但不限于：达梦、Oracle、MySQL 等关系型数据库；Java、Python 等编程语言；以及 Spring Cloud、FastAPI 等主流服务框架。

## 7.6 约束文档生成与打包

平台应生成约束文档集合，约束代码生成智能体在既定模型边界内生成代码，并应支持将本体模型、接口契约、约束文档与需求文档打包下载，供代码生成智能体使用。

## 7.7 模型基线冻结

平台应支持对本体模型进行基线冻结。冻结后的模型版本不得修改；确需变更时，应履行审批流程并生成新版本，同时保留历史基线及其关联产物（物理表、接口契约、约束文档等），以支持追溯与回滚。

# 8 敏态研发功能要求

敏态研发功能实现从模型到可运行智能体的运行时装配，其流程见图 4。

敏态研发流程（装配·运行时）



图 4 敏态研发流程

## 8.1 服务注册

平台应提供服务注册能力，维护真实服务的服务标识与基础地址等信息。服务注册信息宜以服务注册表形式管理。

## 8.2 行为与接口绑定

平台应支持将行为模型中的行为与真实服务接口建立绑定关系。每个行为对应一个接口（含端点、方法与参数），服务标识作为行为与服务之间的关联键。

## 8.3 原子工具生成

平台应依据行为与接口的绑定关系，将单个行为与单个接口一对一封装为原子工具，并注册至工具注册表。原子工具宜采用“行为名\_服务标识\_操作动词”的命名规则，并附加业务域、数据实体、接口版本等标签，以支持检索、分组与权限控制。

## 8.4 组合技能编排

平台应支持将多个原子工具编排为组合技能，编排方案宜由人工智能辅助生成，并支持组合技能的执行。组合技能发布前应经过测试验证与审核确认：测试应覆盖正常路径、异常路径与边界条件；审核宜由具备相应权限的构建人员或业务专家完成；审核通过后方可上线供智能体调用。

## 8.5 智能体与智能助手构建

平台应支持基于统一的运行时内核构建智能体与智能助手。智能体面向开发者与构建者，具备工具调用与任务执行能力；智能助手面向业务用户，偏重领域知识问答与引导。

## 8.6 运行时执行

平台应采用推理-行动-观察（ReAct）循环执行智能体任务，通过流式方式输出执行过程，并对写操作施加护栏约束，记录执行轨迹以支持审计与追溯。执行轨迹留存时长宜不少于 180 天，以满足电网行业安全审计与合规要求；涉密项目应按更高等级要求执行。

## 8.7 装配配置回滚

平台应对敏态装配配置（服务绑定关系、原子工具、组合技能、智能体与智能助手配置等）实行版本化管理，支持在装配失败或运行异常时回滚至上一稳定版本。回滚操作应记录审计日志，并保留回滚前后的配置版本以供追溯。

# 9 数据与接口要求

## 9.1 数据要求

本体模型应采用结构化、可机读且版本可控的描述语言存储；系统数据库与项目业务数据库应实现项目级隔离，宜按项目安全等级采用逻辑隔离或物理隔离；涉密电网项目应采用物理隔离，数据库映射应记录映射规则与置信度标注。

## 9.2 接口要求

平台对外接口宜采用表述性状态传递（REST）风格，统一采用应用编程接口前缀，返回统一结构；人工智能推理过程宜采用服务器发送事件方式进行流式传输。

平台推导的接口契约应为理想契约，其服务标识在真实服务实现前可作为占位符，待真实服务实现后再行绑定。

## 9.3 性能与测试评估要求

平台应具备可量化的性能指标与测试评估方法，性能指标应满足下列要求：

- a) 平台接口调用平均延迟不超过 500ms；
- b) 场景模拟预演并发能力不少于 20 个场景；
- c) 智能体单次任务执行平均耗时（不含人工交互等待时间）不超过 30s；
- d) 系统正常运行时 CPU 平均利用率不超过 70%，内存平均利用率不超过 80%。

测试评估方法应覆盖功能测试、性能测试、接口兼容性测试、安全测试与回归测试；测试环境、测试工具、测试用例与测试数据应形成文档化记录，测试结果应形成测试报告并作为验收依据。

# 10 安全与可信要求

## 10.1 数据安全

平台应保障大语言模型接口密钥等敏感信息的安全存储（宜采用加密方式），并具备结构化查询语言的安全校验能力，禁止执行非查询类语句。平台应对项目数据、业务数据与系统配置数据进行分类分级管理，明确数据访问权限与脱敏规则，防止越权访问与敏感信息泄露。

## 10.2 可信要求

平台应保证所有关键数字由确定性计算产生，大语言模型仅引用而不生成数字；对于基于原始数据经统计口径衍生得到的结果，大语言模型可在明确标注数据来源、计算口径与置信度的前提下生成

衍生结果。每个结果应可溯源至原始查询语句、映射规则与指标口径；数据库映射与人工智能推理均应标注置信度。

### 10.3 护栏

平台应对智能体的写操作实施护栏约束，包括幂等去重、权限校验与失败补偿，防止越权与重复操作。平台还应应对大语言模型的输入 **prompt** 与输出内容实施合规性过滤护栏，识别并拦截敏感信息、违规指令与不符合业务规则的输出，降低敏感信息泄露与恶意利用风险。

### 10.4 AI 安全

平台应建立 AI 安全治理机制，对大语言模型调用进行审计与监控，防范提示注入、模型滥用与未授权访问；宜对模型输出进行事实性校验，避免幻觉导致的错误决策。

### 10.5 模型安全

平台应对使用的本体模型、机器学习模型与大语言模型进行版本管理与完整性校验，防止模型文件被篡改；模型训练与推理过程宜记录数据血缘与模型参数，支持复现与回滚。

### 10.6 内容安全

平台应对生成内容实施安全审查，确保生成的代码、文档、报告与对话回复不包含违法违规、涉密或侵权信息；宜建立内容发布前的审批机制与追溯机制。

## 11 其它功能要求

### 11.1 需求脱敏

平台应具备需求文档脱敏功能，对需求导入与需求文档生成过程中涉及的敏感信息（如个人信息、涉密字段、内部网络地址等）进行自动识别与脱敏处理；脱敏规则应可配置，脱敏记录应可追溯。

### 11.2 模型本地化部署

平台应支持本体模型及平台组件在本地化（私有化）环境中的部署，支持内网或离线环境运行，支持接入本地部署的大语言模型服务；本地化部署环境下模型版本与平台主库的一致性应可校验。

### 11.3 运行态监控与审计

平台应提供运行态监控与审计功能，对智能体运行状态、工具调用、接口访问与异常事件进行实时监控、记录与告警，监控与审计记录留存时长宜不少于 180 天。

### 11.4 知识库管理

平台宜支持领域知识库的构建、维护与版本管理，支持知识条目与本体模型的关联，为智能助手问答与需求分析提供知识支撑。

附录 A  
(资料性)  
本体模型示例

## A.1 概述

本附录给出了本体模型（以 M1 对象模型为例）的结构化描述示意，供理解八模型组织方式参考。

## A.2 M1 对象模型示例

M1 对象模型以 entities 为根键，描述业务实体、属性、关系与约束，示例结构如下：  
entities:

- name: 业务需求简表  
alias: requirementBrief  
description: 提报时同步提交的业务需求简表，使用储备指南统一模板。  
attributes:
  - name: templateVersion  
label: 模板版本  
type: String  
required: true
  - name: userScope  
label: 用户群体及范围  
type: String  
required: true
- relations:
  - target: 需求佐证材料  
type: one-to-many
- constraints:
  - type: FOREIGN\_KEY

其他模型（M2 行为模型、M3 规则模型、M4 场景模型、M5 主体模型、M6 补偿模型、M7 质量模型、ME 事件模型）的组织方式与此类似，分别以 behaviors、rules、scenarios、actors、compensations、quality、events 为根键。

## 参 考 文 献

- [1] 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
  - [2] GB/T 11457—2006 信息技术 软件工程术语
  - [3] GB/T 25069—2022 信息安全技术 术语
  - [4] GB/T 25000.10—2016 系统与软件工程 系统与软件质量要求和评价（SQuaRE） 第10部分：系统与软件质量模型
  - [5] GB/T 25000.51—2016 系统与软件工程 系统与软件质量要求和评价（SQuaRE） 第51部分：就绪可用软件产品（RUSP）的质量要求和测试细则
  - [6] GB/T 35273—2020 信息安全技术 个人信息安全规范
  - [7] GB/T 41373—2022 信息安全技术 网络数据分类分级要求
  - [8] GB/T 41867—2022 信息技术 人工智能 术语
  - [9] GB/T 42018—2022 信息技术 人工智能 平台计算资源 规范
  - [10] GB/T 42131—2022 人工智能 知识图谱技术框架
  - [11] GB/T 43582—2023 信息技术 人工智能 大模型训练与计算能力要求
-