



2026 一带一路暨金砖国家技能发展与技术创新大赛

【AI+应用创新与安全设计赛项】

BRICS2026-ST-143

技术规程

金砖国家工商理事会技能发展、应用技术与创新中方工作组
一带一路暨金砖国家技能发展与技术创新大赛组委会执委会
技术委员会专家组制定

目 录

目录

赛项项目简介	3
1.1 赛项名称	3
1.2 赛项背景与定位	3
1.3 竞赛目的	3
1.4 选手的知识和技能要求	4
二、竞赛内容	5
三、竞赛方式	6
四、竞赛流程	8
五、竞赛试题	11
六、评分方案	12
七、竞赛规则	13
八、技术规范	20
九、竞赛环境、设施和场地	21
十、竞赛设备、工具和材料	22
十一、成绩评定原则、方式和细则	23
十二、奖项设定	25
十三、竞赛组织、安全和后勤保障	26
十四、技能管理与沟通	29
十五、监督、申诉与仲裁	30
十六、竞赛观摩	31
十七、竞赛视频	31
十八、竞赛须知	32

一、赛项项目简介

1.1 赛项名称

中文名称：AI+应用创新与安全设计国际赛

英文名称：AI+ Application Innovation and Security Design
International Competition

赛项类别：电子与信息大类-人工智能类

赛项级别：中国赛区国际赛

赛项组别：中职组、高职组、本科组、教师组/职工组、国际组

1.2 赛项背景与定位

本赛事面向软件技术、人工智能、计算机应用技术、信息安全等相关专业，汇聚国内外优秀团队同台竞技。赛项重点考察选手基于多模型协同，完成行业应用的全流程工程交付能力，并着重评估 AI 应用在数据安全、模型安全、应用安全三个层面的防护设计水平。评审标准同时参照我国国家标准与国际公认的软件工程及 AI 安全规范，确保参赛作品的技术方案具备国际可比性与全球适用性。大赛要求参赛作品必须集成不少于两种不同类型的 AI 模型，构建功能完善、架构成熟、能够有效规避常见网络安全风险的智能应用，最终选拔出开发完备、安全可信、具备全球落地潜力与国际竞争力的 AI 应用创新成果。

1.3 竞赛目的

作为新一轮科技革命的核心技术，人工智能已成为全球科技创新和经

济发展的重要引擎，世界主要国家纷纷将人工智能上升至国家战略层面，加速布局，推动 AI 技术标准国际化与产业智能化深度融合。

在 AI 技术扩散、大模型编程工具全面普及的今天，各行业 AI 应用正在迅速涌现。然而，大量快速生成却未经系统性安全审查的应用，普遍缺乏对网络安全的系统性考量，导致模型数据泄露、API 密钥泄露、提示注入攻击、越权访问等安全事件频发，AI 应用的安全性已从“可选项”升级为“必选项”，成为制约 AI 产业规模化、安全化落地的关键瓶颈。

在金砖国家和“一带一路”倡议背景下，为培养新时代国际化人才，推动全球产业协同发展,促进国际间 AI 应用开发规范与技术标准的交流互通，本届大赛特设“AI+应用创新与安全设计”赛项。赛项聚焦人工智能、计算机应用技术及信息安全相关专业方向，旨在发现和培养一批兼具扎实 AI 开发功底与系统性安全思维的高素质复合型人才，服务全球数字经济的安全、可持续发展。

1.4 选手的知识和技能要求

领域	具体要求
AI 模型认知	了解大语言模型、语音识别、语音合成、视觉识别/分割、图像生成、OCR、异常检测、RAG 等至少 2 类 AI 模型的基本原理、适用场景与调用方式。
编程基础	掌握一门主力开发语言，熟悉 API 调用、JSON 数据处理、前后端交互。

网络与安全基础	理解通信协议、身份认证机制、加密原理、常见 Web 安全风险。
软件工程	了解需求分析、系统设计、模块划分、代码规范、异常处理、容错机制。
AI 编程	整合以上内容,通过提示词制作出具有完善前后端架构、能够解决具体场景痛点的应用,并保证应用安全可用。
国际化协作	能够阅读英文技术文档,使用英文进行项目陈述与答辩(国际队伍)。

二、竞赛内容

赛项以“AI+行业应用”为核心,双重考核参赛选手的工程开发能力与安全防护能力,推动 AI 应用从“能用”向“安全可靠、架构成熟”升级。主要内容如下:

2.1 多模型协同开发与交付

参赛选手须在作品中集成不少于两类 AI 模型,结合真实行业需求完成智能应用的开发与交付。

2.2 AI 应用安全防护

针对当前 AI 应用普遍存在的安全风险,从数据安全、模型安全、应用安全三个维度,为作品构建系统性的安全防护方案。

2.3 评审维度

评审维度从场景功能完备性、AI 模型优化设计、安全防护水平、创新设计水平、展演水平共五个维度进行综合评分。

三、竞赛方式

3.1 竞赛形式与组队

（一）此次竞赛为作品展示赛，作品演示总时长为 15 分钟。

（二）本赛项为团队赛，每支参赛队由 1-3 名选手与 1-2 名指导老师组成。赛事采用国内外队伍统一赛制、分别管理的模式：国内参赛队伍以院校或企业为单位报名参赛，每所院校（含中职、高职、本科）参赛队伍总数不超过 4 支，其中教师组数量不得超过 2 支，中职组、高职组、本科组各自最多可报 4 支但均须在全校总限额内；公司单位参赛队伍总数不超过 2 支，且仅限报名职工组。技工院校、中职、高职、本科院校的全日制在籍学生与在职教师、企业技术人员职工均可报名参赛；国际队伍须为所在国教育机构注册的全日制在籍学生或从事在职教师、企业技术人员工作的在职人员。

（三）参赛选手、指导教师报名获得确认后不得随意更换，如备赛过程中因故无法参赛，须于赛项开赛 10 个工作日前出具盖章的书面申请，经大赛组委会办公室核实后予以更换，否则视为自动放弃竞赛。竞赛开始以后，参赛队不得更换参赛队员。

3.2 竞赛阶段

（一）初赛阶段：由各赛区组委会根据本赛区报名情况组织实施。如

承办校或运营单位因条件所限，确实无法承办线下初赛，大赛组委会将采用线上评审方式，经批准后进行选拔。

各区域选拔赛举办形式以具体区域选拔赛通知为准。

（二）决赛阶段：决赛严格采用线下路演形式进行。入围决赛的队伍须在决赛开赛前一周，将完整项目源代码提交至指定平台。组委会将使用官方代码安全检查工具进行自动化扫描，生成安全评估报告，作为裁判评定的参考依据。每支队伍演示总时长不超过 15 分钟。

总决赛晋级队伍以各区域选拔赛最终表彰文件及晋级名单为准。

3.3 赛区设置

（一）大赛共设置华北、东北、华东、华中、西北、西南、大湾区、东盟八大赛区。根据各赛区参赛队报名情况，组委会将适时启动区域选拔机制；当单个赛区报名队伍数量超过规定限额时，由赛区通过初赛进行选拔，择优晋级决赛。同时鼓励各参赛单位按照大赛通知和技术规程，自行组织校赛进行预选。

（二）大湾区赛区包含广东省、海南省、香港特别行政区及澳门特别行政区。该赛区内港澳地区参赛队伍的报名、初赛及晋级办法参照内地赛区统一执行，如有特殊安排将另行通知。

（三）东盟赛区包含广西壮族自治区及东南亚 10 国（马来西亚、泰国、越南、新加坡、印度尼西亚、菲律宾、缅甸、柬埔寨、老挝、文莱）。广西壮族自治区内院校归入东盟赛区，与东南亚国家队伍同场竞技。

赛区归属表：

赛区	覆盖区域
华北赛区	北京、天津、河北、山西、内蒙古
东北赛区	辽宁、吉林、黑龙江
华东赛区	上海、江苏、浙江、安徽、福建、江西、山东
华中赛区	河南、湖北、湖南
西北赛区	陕西、甘肃、青海、宁夏、新疆、西藏
西南赛区	重庆、四川、贵州、云南
大湾区赛区	广东、海南、香港特别行政区、澳门特别行政区
东盟赛区	广西壮族自治区 + 东盟国家：马来西亚、泰国、越南、新加坡、印度尼西亚、菲律宾、缅甸、柬埔寨、老挝、文莱等国

3.4 决赛规模

决赛规模预计 100-120 支参赛队，每队选手 1-3 名，可指定 1-2 名指导教师，预计参赛总人数约 300 人。该规模包含一定数量的国际参赛队伍（主要来自东盟及“一带一路”沿线国家），国际队伍与国内队伍共同参与决赛评审与奖项评定，不单独设奖。组委会根据实际报名情况动态调整国际队伍名额，确保决赛总规模控制在 100-120 支队伍以内。

四、竞赛流程

4.1 初赛流程

初赛由各赛区竞赛工作组负责组织实施，原则上采用线下集中评审方

式。若赛区承办校或运营单位因条件所限无法承办线下初赛，则由大赛组委会统一采用线上评审方式进行，各赛区须确保初赛按期完成。

（1）赛区启动与通知发布：各赛区竞赛工作组发布初赛通知，明确报名截止时间、作品提交要求及初赛组织形式。

（2）报名与作品提交：参赛队伍在规定时间内完成报名，按照赛区要求提交项目说明书、程序源码、安全架构专项设计说明书材料。

（3）形式审查：赛区竞赛工作组对报名资格和提交材料的完整性、规范性进行审核，公布有效参赛队伍名单。

（4）组织评审：具备线下承办条件的赛区，组织专家进行现场集中评审，可包含作品演示、答辩等环节。条件不具备的赛区，由大赛组委会统一组织线上评审，通过指定平台完成材料审阅、视频评审及线上答辩。

（5）成绩评定与公示：评审专家依据大赛统一技术规程和评分标准打分，确定本赛区晋级国际总决赛的队伍名单，并在指定渠道公示。

（6）晋级名单报备：公示无异议后，各赛区将晋级国际总决赛队伍名单报大赛组委会备案。

4.2 决赛（国际总决赛）流程

决赛即为本届大赛的国际总决赛，由各赛区（华北、东北、华东、华中、西北、西南、大湾区、东盟）晋级的队伍共同参加，严格采用线下路演形式进行。

（1）参赛队报到：各参赛队按规定时间抵达决赛承办地，办理报

到手续，领取参赛证件、资料及赛程安排。

（2）领队会及赛前熟悉场地：召开领队会议，说明竞赛规则、评分标准、赛场纪律及注意事项；会后统一组织参赛队熟悉赛场环境和设备。

（3）开幕式：举办大赛开幕式。

（4）正式比赛：根据抽签顺序，各参赛队依次进入赛场进行作品路演与问辩，每队演示总时长不超过 15 分钟。

（5）安全评估：决赛开赛前一周，各参赛队须将完整项目源代码提交至指定平台，组委会使用官方代码安全检查工具进行自动化扫描，评估报告在路演开始前提供给评委参考。

（6）专家评委评定：评委依据路演表现、作品质量、创新性及安全评估报告等进行综合评分。

（7）成绩评定与公示：全部队伍路演完毕后，组委会汇总、核对并录入成绩，在规定时间内进行成绩公示。

（8）闭幕式暨颁奖仪式：举办闭幕式，宣布获奖名单并颁发奖项。

4.3 决赛时间安排表

具体竞赛时间安排最终以发布的竞赛通知为准，具体竞赛日期及正式比赛组织安排由组委会统一通知发布。

国际总决赛竞赛时间安排与流程（以最终发布通知为准）：

日期	时间	内容
----	----	----

竞赛前一日	08:00-14:00	参赛队报到，安排住宿，领取资料
	14:00-15:00	领队会议、赛项说明会
	15:00-16:00	参观熟悉赛场
	16:00-17:30	大赛开幕式
	17:30	检查封闭赛场
竞赛日	08:00-08:50	竞赛选手检录、身份核验
	08:50-09:00	宣布竞赛注意事项、检查并确认赛位设备、工具及材料
	09:00-12:00	竞赛
	13:30-16:30	竞赛
	16:30-19:00	成绩评定、成绩汇总、成绩核对、录入与解密
	19:00-21:00	成绩公示
竞赛后一日	08:30 - 12:00	闭幕式暨颁奖仪式

五、竞赛试题

5.1 赛题类型与内容

本赛项为开放性命题路演展示赛。参赛队伍自主选择一个真实行业场景，开发集成不少于两类 AI 模型（如大语言模型+视觉识别、语音识别+OCR 等）的智能应用，并从数据安全、模型安全、应用安全三个层面系统落实安全防护设计。最终以“10 分钟演示+5 分钟问答”形式现场展示。

5.2 选题方向

选题方向包括但不限于：智慧教育、智能制造、智慧医疗、数字政务、跨境电商、智慧农业等，鼓励选择具有社会价值或产业落地潜力的细分场景。鼓励国际参赛队伍选择跨国跨境场景，如跨境贸易 AI 合规审查、多语种智能教育平台、国际供应链安全检测等，体现 AI 应用在全球协作中的价值。

5.3 作品约束与提交

模型约束：作品中必须集成至少两种不同类型的 AI 模型，包括但不限于以下模型（本地部署、云端调用均可）：大语言模型（LLM）、语音识别模型（ASR）、语音合成模型（TTS）、视觉识别模型（图像分类、目标检测、分割）、图像生成模型、OCR 文字识别模型、检索增强生成（RAG）模型、推荐/排序模型。

安全要求：要求作品在数据安全、模型安全、应用安全三个维度上体现充分的安全设计，参赛者需深入思考如何为自己的 AI 应用构建有效的安全防护体系。所有核心功能必须现场真实运行演示，不得使用录屏或模拟数据。

竞赛时长与环节：竞赛总时长（含准备、评审、展示与深度问辩）不少于 8 小时。决赛路演环节每队 10 分钟演示+5 分钟问答，严格计时。针对优秀队伍，裁判可增设 10 分钟深度技术问辩，重点考察产品创新、落地规划、安全设计的完整性、模型调优细节及产业落地。决赛前一周集中进行自动化扫描，决赛现场随机抽取 10%队伍进行安全功能实测（5 分钟/队）。

作品提交（比赛开始前一周提交至指定平台）：程序源码、项目作品说明文档、安全架构专项设计说明书。

六、评分方案

6.1 评分原则

遵循“科学严谨、客观公正”原则，采用结果评分+安全扫描评分+现场

路演评分相结合。实行加密评审：参赛队通过抽签获得唯一“参赛编号”，评委仅依据编号评分，直至成绩公布前不得解密。总分相同情况下，依次比较：安全防护水平>场景功能完备性>AI 模型优化设计>创新设计水平>展演水平。

6.2 评分表（满分 100 分）

评分项序号	评分项名称	分值	模块占比
1	场景功能完备性	30 分	30%
2	AI 模型优化设计	20 分	20%
3	安全防护水平	25 分	25%
4	创新设计水平	10 分	10%
5	展演水平	15 分	15%
合计		100	100%

6.3 否决项

集成 AI 模型类型少于 2 种→场景功能完备性子项计 0 分。

未按时提交完整源代码导致无法安全扫描→安全防护水平模块计 0 分。

发现抄袭、套壳、虚假演示→取消评奖资格。

6.4 国际队伍评分说明

国际队伍与国内队伍使用同一套评分标准，合并排名，统一按比例设奖。评委针对英文陈述的队伍配备翻译辅助或由具备双语能力的评委执裁，确保公平。

七、竞赛规则

7.1 参赛选手报名

（1）参赛选手资格：本赛项为团队赛（1-3 人/队），面向国内外高等院校、职业院校的全日制在籍学生及相关专业在职教师、企业技术人员。参赛选手性别不限，年龄不限。国际参赛队伍与国内队伍享有同等竞赛权益与评审标准。每支队伍可指定 1-2 名指导教师。

（2）报名方式：本赛项以院校或企业机构为单位报名参赛，每所院校（含中职、高职、本科）参赛队伍总数不超过 4 支，其中教师组数量不得超过 2 支，中职组、高职组、本科组各自最多可报 4 支但均须在全校总限额内；公司单位参赛队伍总数不超过 2 支，且仅限报名职工组。国际参赛团队可通过大赛国际报名通道提交申请，报名材料须提供中英文双语版本。

（3）资格审查：各参赛报名单位负责本单位参赛人员的资格审查工作，并保存相关证明材料的复印件以备查阅。国际参赛队伍须提供所在院校或机构的在读或在职证明（含英文翻译件），由大赛组委会国际赛事协调组统一核验。

（4）人员变更：参赛选手和指导教师报名获得确认后不得随意更换。如备赛过程中因故无法参赛，须于赛项开赛 10 个工作日前出具书面申请（国际队伍须提交中英文书面申请），经大赛组委会办公室核实后予以更换，否则视为自动放弃竞赛。竞赛开始以后，参赛队不得更换参赛队员。

说明：国际参赛队伍在报名、作品提交及答辩环节可全程使用英文，

大赛组委会提供必要的中英双语赛事文件与技术支持，确保国际选手的参赛体验与评审公平性。

7.2 赛前准备与抽签加密

（1）领队会议与抽签加密：组委会在报到结束后召开领队会议，宣布比赛规定与纪律。会上统一组织抽签，抽取结果将作为该参赛队在比赛全程中的唯一身份标识（序号）。抽签决定路演出场顺序。抽签即加密：抽签产生的序号即为该队的“参赛编号”。抽签完成后，组委会即刻封存序号与真实队名的对应表，交由监督仲裁组保管。直至评分结束前，该表不得公开，确保评委仅依据“参赛编号”进行评分，此为“一次加密”。

（2）熟悉场地与设备调试：组委会统一安排各参赛队有序熟悉场地，并提供统一的设备调试与网络测试时间。参赛队须在规定时段内，在指定区域测试自备笔记本电脑的投影、音响、网络连通性及演示程序运行状况。调试期间，须严格遵守大赛规定：不得进入正式竞赛区，不得摄影摄像，严禁与工作人员进行无关交流，保持安静，严禁拥挤、喧哗、打闹。

7.3 参赛文件提交

参赛队须在正式比赛开始前一周，按组委会要求提交全部电子文件，包括：程序源码、项目作品说明文档（PDF）、安全架构专项设计说明书。所提交的各类文件中，严禁出现学校名称、队名、成员姓名或指导老师姓名等可辨识身份的信息，只能以报名时获得的“参赛编号”署名。逾期未提

交或提交不全、违规署名者，视为放弃参赛资格。组委会将使用官方代码安全检查工具对提交的源代码进行自动化扫描，生成安全评估报告，该报告将直接作为安全防护水平评分的依据。

7.4 比赛入场与身份核验

（1）检录与信息屏蔽：参赛选手须凭参赛证、身份证、学生证（职工组提供工作证明），在正式比赛开始前 30 分钟到达指定地点集合。工作人员将逐一核验选手身份，并核对“参赛编号”。检录后，选手随身物品、服装及自备设备上，凡涉及学校名称、队名、Logo 等可识别身份的信息，均须予以遮盖或移除，否则不予入场。

（2）入场规范：选手按抽签顺序依次入场。正式比赛开始 15 分钟后到场者，视为自动放弃参赛资格，不得入场。比赛结束前 30 分钟起，允许已完成路演的队伍提前离场。

（3）物品携带规定：除比赛禁止的通讯及存储设备外，选手允许携带自备笔记本电脑、纸质材料、产品样品或模型等辅助展示物品上台。所有携带物品同样须遵守信息屏蔽规定。赛场内提供投影、音响等基础展示设施。

7.5 展演与答辩过程

（1）流程与时长：比赛采用“10 分钟演示+5 分钟问答”制。裁判长可依据现场问答情况酌情延长问答时间。计时从选手登台、开始演讲或展示的那一刻起算。演示结束前 1 分钟，工作人员以举牌示意；结束时以倒计时铃声或举牌为终止信号，选手须立即停止展示并进入问答环节。

超时将依据评分标准扣分。

（2）匿名演示规范：选手在演示及答辩全程，只能以“参赛编号”自称，不得透露学校、姓名等任何身份信息，违者按作弊处理。

（3）团队协作与禁止事项：允许队员之间在台上进行正常交流与配合。严禁选手与台下领队、指导教师或助手进行任何形式的手势、举牌、传递信息等互动。领队及指导教师不得陪同上场，须在指定区域就座，全程不得进入赛场进行任何协助。

（4）比赛纪律：选手须听从裁判员统一指挥。演示及问答全程，不得随意离开指定区域或与其他队伍交流。如遇设备或流程问题，须举手向裁判员示意，获得裁判员允许后方可进行处理，否则按作弊行为处理。

（5）故障处理：因选手原因导致展示中断或现场设备损坏，由选手自行承担。因非选手个人因素（如赛场供电、音响投影故障）造成中断，由裁判长视情况裁决，可给予暂停计时或调整至当日最后一位重新展示。

（6）现场秩序：比赛过程中，除裁判员、技术人员、正在进行展示的选手外，其余人员（包括候场选手）未经同意不得进入比赛区域。不设观摩区，参赛队须在指定候场区等候。

7.6 比赛结束与现场收尾

（1）离场确认：路演结束并完成答辩后，选手须将组委会提供的设备复位，整理个人物品。经裁判员检查许可并签字确认后，方得离开

赛场。

（2）物品管控：参赛选手不得将任何与比赛相关的纸质材料、评分表、评委记录等物品带离赛场。选手须配合裁判员做好赛场情况记录，并共同签字确认，不得拒签。

7.7 文明参赛与保密

（1）保密承诺：鉴于路演内容涉及商业创意，所有参赛选手须在赛前签署保密承诺书。

（2）禁止擅自录音录像：赛场内严禁选手及观众自行进行录音、录像或直播，以防创意泄露。

（3）信息发布与采访纪律：任何选手未经赛项组委会批准，不得接受任何单位和个人的采访，不得在比赛期间及成绩公布前，擅自通过网络、媒体等任何渠道发布比赛相关信息。违反者，视情节严重程度，给予取消比赛资格、取消竞赛成绩并通报批评的处罚。

（4）媒体入场：新闻媒体人员进入赛场，必须经过赛点领导小组的明确允许，并听从现场工作人员安排，不得影响竞赛正常进行。

（5）选手离场管理：比赛期间，选手不得擅自离开指定区域，遇特殊情况须经裁判员同意。选手饮水、上洗手间等，统一计入比赛用时，不另作安排。

（6）信息传递：非同队选手之间，不得以任何方式传递信息，如传递纸条、手势、口头传话等。

（7）其他事项：其他未涉及事项或突发事件，由大赛组委会负责

解释或决定。

7.8 技术核验机制

（1）模型集成核验：现场核对系统模型调用链路与文档描述一致性，确认模型类型不少于 2 种。

（2）安全扫描复验：组委会基于已提交的源代码运行官方安全检查工具，现场展示安全报告，并对扣分项进行核实。

（3）安全功能实测：现场验证权限控制、数据防护、AI 接口管控、日志审计功能真实可用，全程不开展破坏性攻击测试。

（4）代码与演示一致性检查：随机抽取功能点，核对演示内容与源代码实现是否一致，防止演示造假。

7.9 成绩评定与公布

（1）评分构成：评委根据评分标准，依据参赛队的“参赛编号”进行独立评分，评分维度综合参考：现场路演表现（项目阐述、应用价值、功能完备度等）、技术报告质量（架构设计、创新性、文档规范性等）、网络安全检测报告（由技术组提供的专业检测结果）。

（2）评分方式：赛后由组委会汇总各评委的评分，计算算术平均分作为最终成绩。

（3）成绩解密与复核：监督仲裁组对全部成绩复核无误后，启封“参赛编号与真实队名对应表”，完成成绩解密，将编号成绩映射为各队的最终成绩。对存在争议的评分，由仲裁组启动复核程序，其裁决为最终决定。国际队伍的参赛编号与真实队名对应表同样由监督仲裁组封存，

解密后成绩合并入总排名。

（4）成绩公布：经裁判长、监督仲裁组签字确认的最终成绩单，由承办单位信息员录入并打印。成绩将在闭幕式上统一公布，此时公布队名及对应成绩。

（5）公示与申诉流程：成绩公布后，设 2 小时现场公示期。公示期内，对成绩有异议的参赛队，可由领队向监督仲裁组提交书面申诉，仲裁组的裁决为最终决定。超过公示期不再受理任何申诉。

八、技术规范

本技术规范为“AI+应用创新与安全设计赛项（中国赛区国际赛）”的评分依据，面向全球参赛团队，以开放融合的视角评审参赛作品的开发规范性、技术成熟度与安全防护能力。标准体系由我国国家标准与国际公认标准共同构成，涵盖软件工程过程规范、人工智能应用开发规范及人工智能应用安全三大领域。国内外标准的有机融合，确保参赛作品既能满足本土合规要求，又能充分对标国际通行的开发规范与安全准则，切实契合本赛项“中国赛区国际赛”的权威评审定位。

8.1 软件工程与过程规范

序号	标准号	中文标准名称
1	GB/T 8566-2022	系统与软件工程 软件生存周期过程
2	GB/T 8567-2006	计算机软件文档编制规范
3	GB/T 31102-2025	系统与软件工程 软件工程知识体系
4	GB/T 15532-2008	计算机软件测试规范
5	ISO/IEC/IEEE 12207:2017	系统与软件工程 软件生存周期过程
6	ISO/IEC/IEEE 29148:2018	系统与软件工程 生存周期过程 需求工程
7	ISO/IEC 25010:2011	系统与软件工程 系统与软件质量模型

8.2 人工智能应用开发规范

序号	标准号	中文标准名称
1	GB/T 41867-2022	信息技术 人工智能 术语
2	GB/T 43782-2024	人工智能 机器学习系统技术要求
3	GB/T 45288.1-2025	人工智能 大模型 第1部分：通用要求
4	GB/T 45288.2-2025	人工智能 大模型 第2部分：评测指标与方法
5	GB/T 45225-2025	人工智能 深度学习算法评估
6	GB/T 45628-2025	人工智能 知识图谱 知识交换协议
7	ISO/IEC 22989:2022	信息技术 人工智能 概念与术语
8	ISO/IEC 23053:2022	信息技术 人工智能 使用机器学习的 AI 系统框架
9	ISO/IEC 42001:2023	信息技术 人工智能 管理体系

8.3 人工智能应用安全规范

序号	标准号	中文标准名称
1	GB/T 45654-2025	网络安全技术 生成式人工智能服务安全基本要求
2	GB/T 45958-2025	网络安全技术 人工智能计算平台安全框架
3	GB 45438-2025	网络安全技术 人工智能生成合成内容标识方法
4	GB/T 46796-2025	数据安全技术 数据接口安全风险监测方法
5	GB/T 45392-2025	数据安全技术 基于个人信息的自动化决策安全要求
6	GB/T 22080-2025	网络安全技术 信息安全管理体系 要求
7	ISO/IEC 27001:2022	信息安全、网络安全和隐私保护 信息安全管理体系 要求
8	ISO/IEC 23894:2023	信息技术 人工智能 风险管理指南
9	ISO/IEC 27701:2019	隐私信息管理体系 要求和使用指南

九、竞赛环境、设施和场地

（一）竞赛场地应为地面平整、通风、明亮的室内场地，场地面积不小于 400 平方米（可根据参赛队数量调整），净高不低于 3.5 米，保证赛场采光（大于 500lux）、照明和通风良好。

（二）场地应划分明确的功能区域，至少包含：路演展示区、参赛队

伍候场区、评委工作区和技术支持区。各区域之间应保持适当间距，避免相互干扰。

（三）路演展示区应配备：高亮度投影仪或大型 LED 显示屏，分辨率不低于 1080P，确保演示内容清晰可见；音响系统（含无线麦克风不少于 2 支），保障选手讲解与评委提问的语音清晰；演示操作台及电源接口，可供选手放置自备笔记本电脑并连接投影；计时提示设备（电子倒计时屏或提示牌），用于演示时间提醒。

（四）参赛队伍候场区应配备足够数量的座椅，供候场选手和指导教师休息等候，并设置清晰的叫号提示。

（五）评委工作区应配备桌椅、评分终端（计算机或平板设备）、有线网络接口及电源，供评委实时记录评分。

（六）整个竞赛场地应提供稳定的有线网络接口和无线网络覆盖，供选手演示时调用云端 AI 模型及访问网络资源。

（七）竞赛场地设置服务区，提供医疗、饮水等基本服务保障。技术支持区为选手提供投影转接、网络应急等必要协助。

（八）场地布置须设置明确的疏散通道，并在墙面显著位置张贴安全疏散路线示意图。

十、竞赛设备、工具和材料

本赛项采用选手自带设备与赛场基础环境相结合的模式，不再指定特定品牌的技术平台。

10.1 选手自备设备

参赛队须自带满足开发与演示需求的笔记本电脑（每人可带 1 台），操作系统不限。必须预装所需开发环境、模型调用工具、演示辅助软件。禁止携带独立通讯设备（手机需调至静音并存放于指定区域）。

10.2 赛场基础环境

设备/环境	规格要求
路演显示	高亮度投影仪或 LED 大屏（分辨率 $\geq 1080P$ ）
音响系统	含无线麦克风不少于 2 支
演示操作台	配备电源接口、HDMI/VGA 转接头
计时设备	电子倒计时屏或提示牌（中英文显示）
网络环境	稳定有线网络接口+无线 WiFi 覆盖（支持国际访问）
安全检测服务器	预置官方代码安全检查工具，支持代码上传与自动化扫描

10.3 竞赛平台与工具

报名平台：中英双语界面，支持国际队伍注册、资料上传、状态查询。
代码安全检测平台：中英双语操作界面，可生成英文版安全评估报告。

10.4 国际队伍特殊支持

赛场提供多标准电源转换插头。现场技术支持团队可提供英文在线翻译服务。必要时可协助国际队伍进行网络环境调试，确保云端 AI 模型调用稳定。

十一、成绩评定原则、方式和细则

11.1 评分标准制定原则

赛项围绕人工智能应用开发与安全设计相关行业规范和岗位技能、院

校专业教学规律、相关专业教学标准设置考核内容并制定评分标准。赛项采用结果评分、安全扫描评分与现场路演评分相结合的方式，本着“科学严谨、客观公正”的原则，重点考察作品的场景功能完备性、AI 模型优化设计水平、安全防护水平、创新设计水平及现场路演表现。

11.2 评分方法

赛项采取分步得分、累计总分的计分方式。各评分项目间分别计算得分，项目间错误不传递。竞赛总分按百分制计分。

赛项采取加密评审原则。参赛队报到后，由加密裁判组织抽签，抽取的序号即为该队“参赛编号”，同时决定路演出场顺序。抽签完成后，编号与队名对应表即刻封存，交由监督仲裁组保管，直至评分结束前不得公开，确保评委仅依据“参赛编号”按照“按出场顺序依次评审”进行评分，确保成绩评定客观、严谨、准确。

裁判长正式提交评分结果并复核无误后，在监督仲裁组的监督下启封“参赛编号与真实队名对应表”，完成成绩解密。

如出现参赛队总分相同情况，按照评分项目的得分高低依次排序：总分相同比较“安全防护水平”得分，高者优先；如仍相同，比较“场景功能完备性”得分；以此类推，依次按“AI 模型优化设计”、“创新设计水平”、“展演水平”进行排序。如所有项目成绩均相同，由裁判组全体人员根据作品整体表现进行裁定。

竞赛过程中，参赛选手如出现扰乱赛场秩序、干扰裁判正常工作等不文明行为的，由裁判长扣减相应分数，情节严重的取消竞赛资格，竞赛成

绩为 0 分，队员退出比赛现场。参赛选手不得在提交的任何材料或现场展示内容中标注含有本参赛队身份信息的记号，如有发现，取消评奖资格。

11.3 评分细则

作品评审与路演展示，满分 100 分。竞赛评分见下表：

评分模块	评分子项序号	评分子项名称	分值	模块占比
作品综合评审	1	场景功能完备性	30 分	30%
	2	AI 模型优化设计	20 分	20%
	3	安全防护水平	25 分	25%
	4	创新设计水平	10 分	10%
	5	展演水平	15 分	15%
合计			100	100%

11.4 安全防护水平分说明

此项评分基于安全报告，该报告由官方代码安全检查工具对赛前提交的源代码进行自动扫描后生成，结合现场核验情况进行评分。

十二、奖项设定

以参赛队最终比赛成绩为依据，依据四舍五入的原则，设一等奖占比 10%，分别颁发金牌及证书；二等奖占比 20%，分别颁发银牌及证书；三等奖占比 30%，分别颁发铜牌及证书；其他选手颁发优秀奖证书。

获得一等奖、二等奖队伍的指导教师颁发优秀指导教师证书。

获得一等奖的参赛单位颁发最佳组织奖证书；获得二等奖的参赛单位

颁发优秀组织奖证书。

另设竞赛支持奖、突出贡献奖、赛项组织贡献奖若干名，颁发给各竞赛平台支持单位、竞赛承办单位，按类别颁发证书、奖牌。

十三、竞赛组织、安全和后勤保障

13.1 组织机构

在赛项组委会的领导下成立由专家组、裁判组、监督仲裁组和竞赛办公室组成的比赛管理组织机构。具体要求与分工如下：

（1）专家组：负责制定竞赛规程、技术文件、赛题库等相关工作。

（2）裁判组：实行“裁判长负责制”，设裁判长1名，全面负责赛项的裁判与管理工作，并处理竞赛过程中出现的争议问题。裁判员根据比赛工作需要分为加密裁判和评分裁判。加密裁判负责组织参赛选手抽签，并对参赛选手的信息进行加密、解密，不参与评分工作。评分裁判负责对参赛选手的技能展示、操作规范和竞赛作品等按赛项评分标准进行评定。

（3）监督仲裁组：负责对裁判组的工作进行全程监督，并对竞赛成绩抽检复核。负责受理参赛队领队提出的对裁判结果的书面申诉并及时反馈复议结果。

（4）竞赛办公室：在竞赛组委会的领导下，负责赛项的组织安排，总体协调日常管理工作。主要包括制定竞赛的具体组织方案及实施计划，并组织和监督实施；负责与竞赛各相关单位的日常沟通和协调；负责竞

赛期间的各项宣传工作；负责竞赛奖品、物品的设计、制作和管理；负责竞赛经费的筹措、使用和管理；负责竞赛的总结和统计分析等。竞赛办公室下设综合协调组、宣传组、志愿者服务组、后勤保障组、安全保卫组等。

13.2 安全保障

1. 设置赛项安全保障组，组长由赛项组委会主任担任。赛项安全保障组成员由各赛场安全责任人担任。每一赛场指定一名安全责任人，对本赛场的安全负全责，在发生意外情况时负责调集救援队伍和专业救援人员，安排场内人员疏散工作。

2. 赛项组委会赛前组织专人对比赛现场、住宿场所和交通保障进行考察，对安全工作提出明确要求。承办院校赛前按照赛项组委会要求排除安全隐患。

3. 建立与公安、消防、司法行政、交通、卫生、食品、质检等相关部门的协调机制，保证比赛安全，制定应急预案，及时处理突发事件。设置医护人员、消防人员和保安人员的专线联系人，由赛场安全负责人对口联系。

4. 赛场的布置，赛场内的器材、设备符合国家有关安全规定，竞赛设备和设施安装严格按照安全施工标准施工，电源布线、电器安装按规范施工。竞赛前进行赛场仿真模拟测试，以发现可能出现的安全问题。

5. 各竞赛工位竞赛设备使用独立的电源，保障安全。竞赛选手在调试演示程序时应及时保存，避免突然停电造成数据丢失。

6. 按防火安全要求配置灭火器，并指定赛场安全责任人在紧急时候使用。

7. 赛场周围设立警戒线，防止无关人员进入发生意外事件。

8. 场地布置划分区域，按安全要求设定疏散通道，并在墙面显著位置张贴安全疏散通道和路线示意图。如果出现安全问题，在赛场安全负责人的指挥下，迅速按紧急疏散路线撤离现场。

9. 比赛期间所有进入赛区的车辆、人员需凭证入内，并主动向工作人员出示有效证件。

10. 赛项组委会会同承办院校在赛场人员密集、车流人流交错的区域，设置齐全的指示标志、增加引导人员，同时开辟备用通道。

13.3 后勤保障

1. 竞赛期间，由赛项承办院校统一安排参赛选手和指导教师的食宿。承办院校须尊重少数民族参赛人员的宗教信仰及文化习俗，根据国家相关的民族、宗教政策，安排好少数民族参赛选手和教师的饮食起居。

2. 竞赛期间，安排的住宿地要求具有宾馆、住宿经营许可资质。

3. 竞赛期间，有组织的参观活动的交通安全由赛区组委会负责。赛项组委会和承办院校须保证比赛期间选手、指导教师和裁判员、工作人员的交通安全。

4. 除必要的安全隔离措施外，严格遵守国家相关法律法规，保护个人隐私和人身安全。

13.4 参赛队职责

1. 各参赛单位在组织参赛队时，须安排为参赛选手购买大赛期间的人身意外伤害保险。
2. 各单位参赛队组成后，须制定相关管理制度，并对所有参赛选手、指导教师进行安全教育。
3. 各参赛队伍须加强参赛人员的安全管理，并与赛场安全管理对接。
4. 参赛队如有车辆，一律凭大赛组委会核发的车辆证件出入校门，并按指定线路行驶，按指定地点停放。

十四、技能管理与沟通

14.1 报名与资格审查

国内队伍通过大赛官网报名；国际队伍通过国际报名通道（中英双语）提交。国际队伍需提供所在院校/机构的在读或在职证明（含英文翻译件）。报名平台与安全核查提交平台均支持中英双语操作界面。

14.2 赛前沟通与培训

赛前 1-2 个月举办线上双语公开课，内容包括：规程解读、安全开发规范、多模型集成技术、安全检测工具使用。设立双语技术支持群组，为国际队伍提供时差友好的咨询窗口。

14.3 抽签与加密

领队会上统一抽签，决定“参赛编号”和路演出场顺序。抽签即加密，对应表由监督仲裁组封存，评分结束后解密。

14.4 现场管理与秩序

选手凭有效证件入场，全程仅以参赛编号自称，不得透露身份信息。赛场不设观摩区，全程录像监控。严禁选手与场外指导老师或助手互动，违规者按作弊处理。

14.5 成绩公示与申诉

决赛当日设 2 小时现场成绩公示期（中英文双语公示）。申诉须由领队提交书面报告（中英文均可），监督仲裁组 2 小时内组织复议并书面答复。

14.6 国际队伍特别沟通

组委会提供英文版《参赛指南》《赛场行为准则》《常见问题解答》。配备具备国际竞赛组织经验的双语志愿者和工作人员。

十五、监督、申诉与仲裁

1. 本赛项在竞赛过程中若出现有失公正或有关人员违规操作等现象，各参赛队可在成绩公布后 2 小时现场公示期内向赛项监督仲裁组提出申诉，超过时效将不予受理。

2. 申诉时，应按照规定程序由参赛队领队向赛项监督仲裁组递交亲笔签字同意的书面申诉报告，报告中应对申诉事件的现象、发生时间、涉及人员、申诉依据等进行充分、实事求是的叙述，非书面申诉不予受理。

3. 赛项监督仲裁组在接到申诉报告后的 2 小时内组织复议，并及时将复议结果以书面形式告知申诉方。不受理申诉的，须说明理由。

4. 仲裁结果由申诉人签收，不能代收，如在约定时间和地点申诉人离开，视为自行放弃申诉。

5. 申诉方不得以任何理由拒绝接收仲裁结果，不得以任何理由采取过激行为扰乱赛场秩序，否则视为放弃申诉。申诉人对仲裁结果不满意的，可向赛项组委会仲裁委员会提出复议申请。

6. 申诉方可随时提出放弃申诉。

十六、竞赛观摩

1. 竞赛现场全过程监控录像，记录赛场全过程。为避免影响选手参赛，不设观摩区。

2. 在赛场外布置开放式展区，对人工智能技术进行相关科普宣传，将人工智能在人们生活中的应用或者未来生活的应用对公众进行展现。

十七、竞赛视频

本赛项将指定工作人员进行摄录和后期视频处理工作，摄录内容包括赛项开闭幕式、比赛全过程、获奖作品和专家的点评，并适时对参赛人员、裁判员、获奖参赛队、优秀指导教师、行业和企业专业人员进行采访，采访内容包括选手参赛情况、裁判和工作人员工作情况、获奖参赛队获奖感言及赛事发展与行业前景。

摄录视频将按内容不同分别在大赛官方、主流视频网站（如优酷）、教学资源转化的多媒体光盘和网站（空间）上发布和收录，供大赛宣传、教师查阅、教学和学生使用。

十八、竞赛须知

18.1 参赛队须知

1. 参赛队名称：统一使用院校代表队的名称。

2. 参赛队组成：每支参赛队为 1-3 名符合参赛资格的选手，每支参赛队可指定 1-2 名指导教师，参赛选手和指导教师均须经报名并通过资格审查后确定。

3. 各参赛队在报到时，请出示为参赛选手购买的大赛期间的人身意外伤害保险。如未购买，将暂时不予办理报到手续，将直接影响选手参赛资格。

4. 参赛队选手和指导教师要有良好的职业道德，严格遵守比赛规则和比赛纪律，服从裁判，尊重裁判和赛场工作人员，自觉维护赛场秩序。

5. 比赛进行过程中及不同的赛段，参赛队不可以更换参赛选手。赛前 10 个工作日内可申请更换，此后不允许。允许指导教师缺席。

18.2 指导教师须知

1. 各参赛队要发扬良好道德风尚，听从指挥，服从裁判，不弄虚作假。如发现弄虚作假者，取消参赛资格，取消竞赛成绩，名次无效。

2. 各代表队领队要坚决执行竞赛的各项规定，加强对参赛人员的管理，做好赛前准备工作，督促选手带好证件等竞赛相关材料。

3. 竞赛过程中，除参加当场次竞赛的选手、现场技术人员和经批准的人员外，领队、指导教师及其他人员一律不得进入竞赛现场。指导教师须在指定候场区就座。

4. 参赛代表队若对竞赛过程有异议，在规定的时间内由领队向赛项监督仲裁组提出书面报告。对申诉的仲裁结果，领队要带头服从和执行，并做好选手工作。参赛选手不得因申诉或对处理意见不服而停止竞赛，否则以弃权处理。

5. 指导教师应及时查看大赛专用网页中有关赛项的通知和内容，认真研究和掌握本赛项竞赛的规程、技术规范和赛场要求等文件，指导选手做好赛前的一切技术准备和竞赛准备。

6. 领队和指导教师应在赛后做好赛事总结和工作总结。

18.3 参赛选手须知

1. 参赛选手严格遵守赛项规章、安全操作规程和工艺准则，保证人身及设备安全，接受裁判员的监督和警示，文明竞赛，一旦出现较严重的安全事故，经裁判长批准后将立即取消其参赛资格。

2. 参赛选手应按有关要求如实填报个人信息，否则取消竞赛资格。

3. 参赛选手凭统一印制的参赛证和有效身份证件参加竞赛，按赛项规定的时间、顺序、地点参赛。

4. 参赛选手应认真学习领会本次竞赛相关文件，自觉遵守大赛纪律，服从指挥，听从安排，文明参赛。

5. 参赛选手可携带自备笔记本电脑及必要的演示辅助物品进入赛场，严禁携带与竞赛无关的通讯设备进入展示区。

6. 竞赛时，在收到开赛信号前不得启动演示操作，各参赛队自行决定队内分工与展示流程，按抽签顺序在指定展示区内完成路演展示，严

禁作弊行为。

7. 竞赛完毕，选手应全体起立，结束展示。将自备设备及物品整理带离，经工作人员确认后，方可离开赛场。离开赛场时不得带走赛场的任何资料和设备。

8. 在竞赛期间，未经组委会的批准，参赛选手不得接受其他单位和个人进行的与竞赛内容相关的采访。参赛选手不得擅自公布竞赛的相关信息。

9. 各竞赛队按照大赛要求提交竞赛成果，禁止在竞赛成果上做任何与竞赛无关的记号。按照程序提交竞赛结果，并与裁判一起签字确认。

18.4 工作人员须知

1. 服从赛项组委会的领导，遵守职业道德、坚持原则、按章办事，切实做到严格认真，公正准确，文明执裁。以高度负责的精神、严肃认真的态度和严谨细致的作风做好工作。

2. 熟悉竞赛规则，认真执行竞赛规则，严格按照工作程序和有关规定办事。佩戴裁判员胸卡，着裁判员服装，仪表整洁，语言举止文明礼貌，接受仲裁工作组成员和参赛人员的监督。须参加赛项组委会的赛前执裁培训。

3. 竞赛期间，保守竞赛秘密，不得向各参赛队领队、指导教师及选手泄露、暗示大赛秘密。

4. 严格遵守比赛时间，不得擅自提前或延长。严格执行竞赛纪律，不得向参赛选手暗示解答与竞赛有关的问题，更不得向选手进行指导或

提供方便。

5. 实行回避制度，不得与参赛选手及相关人员接触或联系。

6. 坚守岗位，不迟到，不早退。监督选手遵守竞赛规则和安全操作规程的情况，不得无故干扰选手比赛，正确处理竞赛中出现的问题。

7. 遵循公平、公正原则，维护赛场纪律，如实填写赛场记录。

18.5 国际参赛队须知

1. 国际队伍须自行办理来华签证及保险，组委会可提供官方邀请函。

2. 参赛的国际队伍须在赛前完成材料的双语改造，确保路演流畅。

3. 作品内容不得违反参赛者所在国及中国的法律法规，不得包含敏感政治、宗教、种族等内容。