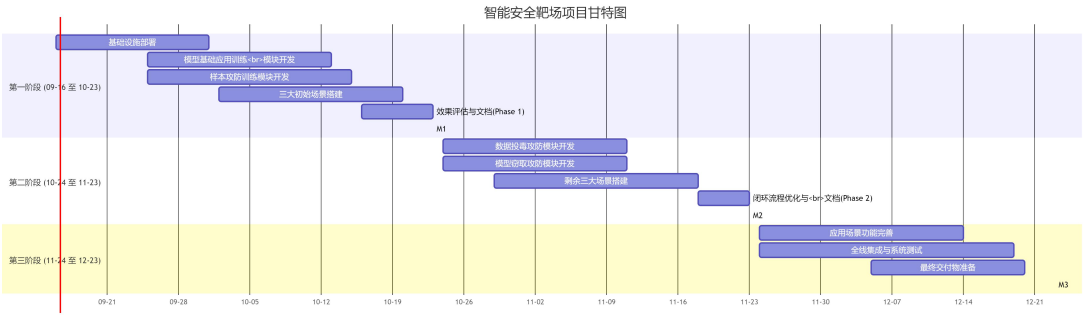
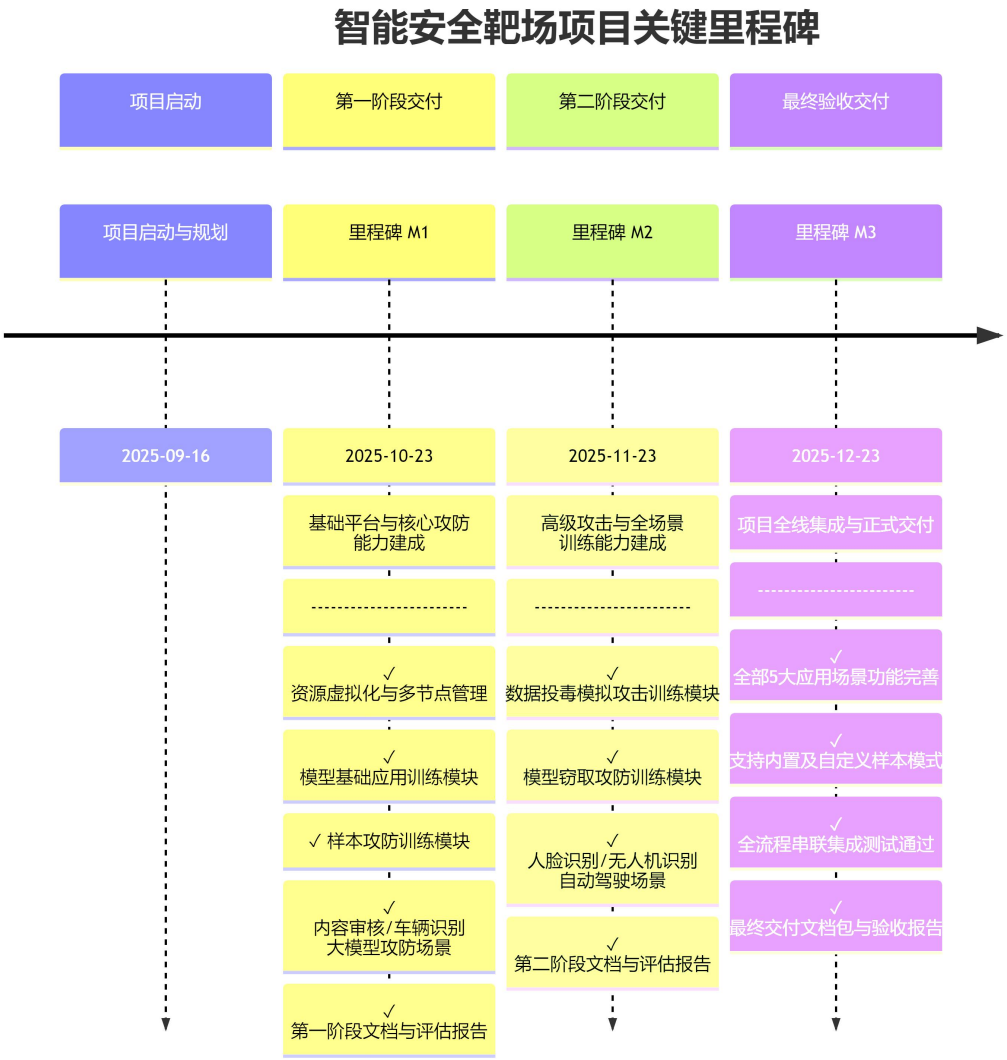
本项目计划分为三个阶段实施，以确保项目有序推进、风险可控、成果可测。每个阶段均设置明确的里程碑交付物，并与招标文件的技术要求条款严格对应。

1. 总体里程碑概览

里程碑编号	里程碑名称	计划完成日期	核心交付物与验收标准
M1	基础平台与核心攻防能力建成	2025-10-23	1. 完成资源虚拟化与多节点管理平台部署。 2. 完成模型基础应用训练、样本攻防训练模块开发，并通过验收。 3. 完成内容审核、车辆识别、大模型攻防三个场景的初步搭建与闭环流程验证。 4. 交付第一阶段所有文档。
M2	高级攻击与全场景训练能力建成	2025-11-23	1. 完成数据投毒、模型窃取两大高级攻防训练模块开发，并通过验收。 2. 完成人脸识别、无人机识别、自动驾驶三大场景的攻防训练功能开发。 3. 所有训练场景均实现攻击->防御->评估->教学的闭环流程。 4. 交付第二阶段所有文档。
M3	项目全线集成与正式交付	2025-12-23	1. 全部 5 个应用场景功能完善，均支持内置及自定义样本模式。 2. 所有功能模块集成完毕，全流程串联测试通过，系统达到上线标准。 3. 交付最终版全部项目文档、操作手册及培训材料。 4. 项目最终验收。



项目甘特图
(Gantt Chart) - 优



智能安全靶场项目
里程碑图 .png

2. 详细工作计划

（一）第一阶段：基础平台与核心攻防能力建设（2025.09.16 - 2025.10.23）

阶段目标：搭建系统基础架构，实现资源虚拟化管理，并完成样本攻防等核心模块的开发与初步集成。

WBS编号	工作内容	详细任务描述	关联技术标准条款	输出物/验收标准
1.1	**基础设施部署**	1. 完成GPU服务器资源池化与虚拟化部署。 2. 安装部署操作系统及容器化管理平台。 3. 实现多计算节点的统一管理和资源调度。	(一)1.(4), (6)	1. 可用的虚拟化资源平台。 2. 多节点管理平台操作手册。
1.2	**模型基础应用训练模块开发**	1. 开发算法上传、数据选择、训练、发布等功能。 2. 开发模型优化、代码编辑等功能。 3. 开发大模型Prompt编辑、输入输出测试界面。	(一)2.(1), (2), (3)	1. 功能完整的模型训练与测试Web界面。 2. 配套训练案例及指导书。
1.3	**样本攻防训练模块开发**	1. 集成≥10种样本攻击算法（FGSM, PGD, CW等）。 2. 集成≥5种训练防御方法和≥3种样本检测方法。 3. 开发攻击成功率、准确率下降等评估指标展示功能。	(一)3.(1), (2), (3); (二)2.(1), (2), (3), (4)	1. 可运行的样本攻防训练模块。 2. 攻击与防御算法清单及测试报告。
1.4	**三大初始场景搭建**	1. **内容审核场景**：集成靶标模型、数据集；实现文本攻防技能。 2. **车辆识别场景**：集成YOLO等模型、KITTI等数据集；实现图像攻防技能。 3. **大模型攻防场景**：集成Qwen2, ChatGLM等模型；实现DAN攻击等技能。	(一)7.(3), (4), (6); (二)6.(3)-(6)	1. 三个场景的可运行环境。 2. 各场景配套的数据集、模型、技能清单。
1.5	**效果评估与文档**	1. 实现第一阶段各模块的评估维度和指标展示。 2. 编写并提交第一阶段交付文档（设计、测试报告等）。	(一)8.(1)	1. 系统评估报告。 2. 第一阶段所有交付

WBS编号	工作内容	详细任务描述	关联技术标准条款	输出物/验收标准
				文档。

（二）第二阶段：高级攻击与全场景训练能力建设（2025.10.24 - 2025.11.23）

阶段目标：开发数据投毒、模型窃取等高级攻击模块，并完成剩余所有应用场景的深度集成。

WBS编号	工作内容	详细任务描述	关联技术标准条款	输出物/验收标准
2.1	**数据投毒攻防模块开发**	1. 集成数据中毒和模型注入型后门攻击方法≥8种。 2. 集成投毒防御算法（如NC, STRIP）≥3种。 3. 开发投毒攻击成功率、模型性能影响等评估功能。	(一)4.(1), (2); (二)3.(1)-(5)	1. 可运行的数据投毒攻防训练模块。 2. 攻防算法清单及测试报告。
2.2	**模型窃取攻防模块开发**	1. 集成模型模拟、输出逆向等窃取攻击类型≥3种。 2. 集成API限制、噪声注入等防御措施≥3种。	(一)5.(1), (2), (3); (二)4.(1), (2)	1. 可运行的模型窃取攻防训练模块。 2. 攻防方法清单及测试报告。
2.3	**剩余三大场景搭建**	1. **人脸识别场景**：集成ArcFace等模型、LFW等数据集；实现躲避/假冒攻防技能。 2. **无人机识别场景**：集成Drone-YOLO模型、专用数据集；实现图像攻防技能。 3. **自动驾驶场景**：集成UniAD等模型、Cityscapes等数据集；实现定向攻防技能。	(一)7.(2), (5), (6); (二)6.(1), (2), (7)-(10)	1. 三个场景的可运行环境。 2. 各场景配套的数据集、模型、技能清单。

WBS编号	工作内容	详细任务描述	关联技术标准条款	输出物/验收标准
2.4	**闭环流程优化与文档**	1. 确保所有新模块和新场景均融入“攻击-防御-评估-教学”闭环。 2. 编写并提交第二阶段交付文档。	(一)1.(4), (6); (一)8.(1)	1. 全流程集成测试报告。 2. 第二阶段所有交付文档。

（三）**第三阶段：全线集成与交付（2025.11.24 - 2025.12.23）**

阶段目标：完成所有功能的集成测试，完善应用场景，支持自定义数据，准备项目最终验收。

WBS编号	工作内容	详细任务描述	关联技术标准条款	输出物/验收标准
3.1	**应用场景功能完善**	1. 对 5 大应用场景进行全面测试和功能增强。 2. 为所有场景开发**自定义样本数据**上传、标注、应用功能。	(一)7.(1)	1. 5 个功能完整且稳定的应用场景。 2. 每个场景均支持内置和自定义样本模式的测试报告。
3.2	**全线集成与系统测试**	1. 进行系统全功能、全流程的串联测试，确保无缝衔接。 2. 性能、压力、安全性和用户体验优化。	(一)1	1. 全线集成测试报告。 2. 系统性能优化报告。
3.3	**最终交付物准备**	1. 整理并提交全部甲方要求的最终交付文档。 2. 准备系统部署手册、用户操作手册、培训材料等。	N/A	1. 完整的最终交付文档包。 2. 最终版的系统评估维度、指标和结果报告。
3.4	**项目验收**	1. 与甲方共同进行系	N/A	1. 甲方签署的项目验

WBS 编号	工作内容	详细任务描述	关联技术标准条款	输出物/验收标准
		统演示和功能验证。 2. 解决验收过程中发现的任何问题。 3. 完成项目最终验收。		收报告。

备注：

带“★”条款：计划中所有工作内容均旨在满足技术标准中的关键条款（带★），请在每个里程碑验收时逐一核对。

风险管理：建议每周召开项目例会，同步进度并识别风险（如算法实现难度大、算法集成难度大、阶段性延期等），及时制定应对策略。

质量保障：每个开发模块都必须经过单元测试、集成测试和 UAT（用户验收测试），确保交付质量。