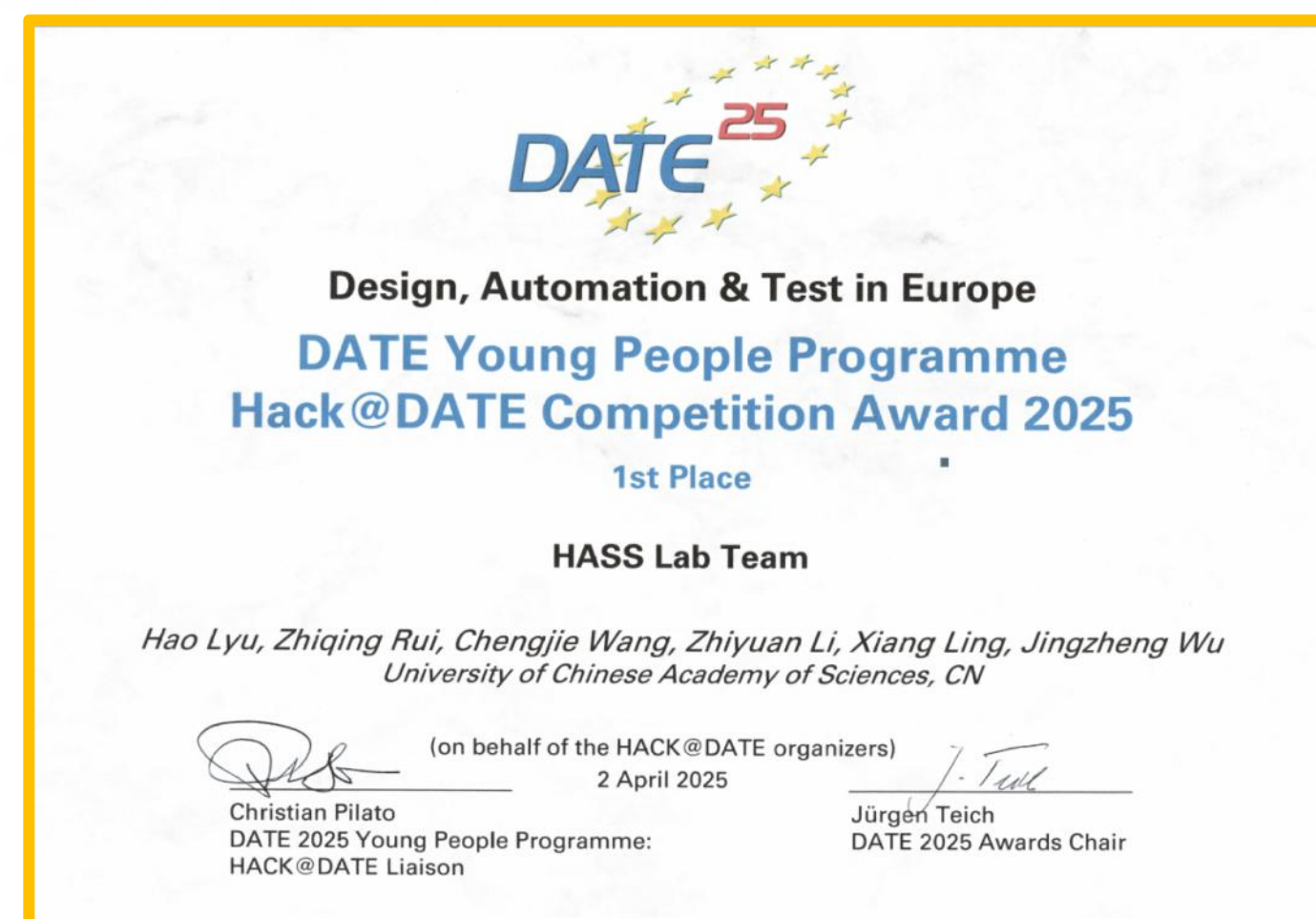


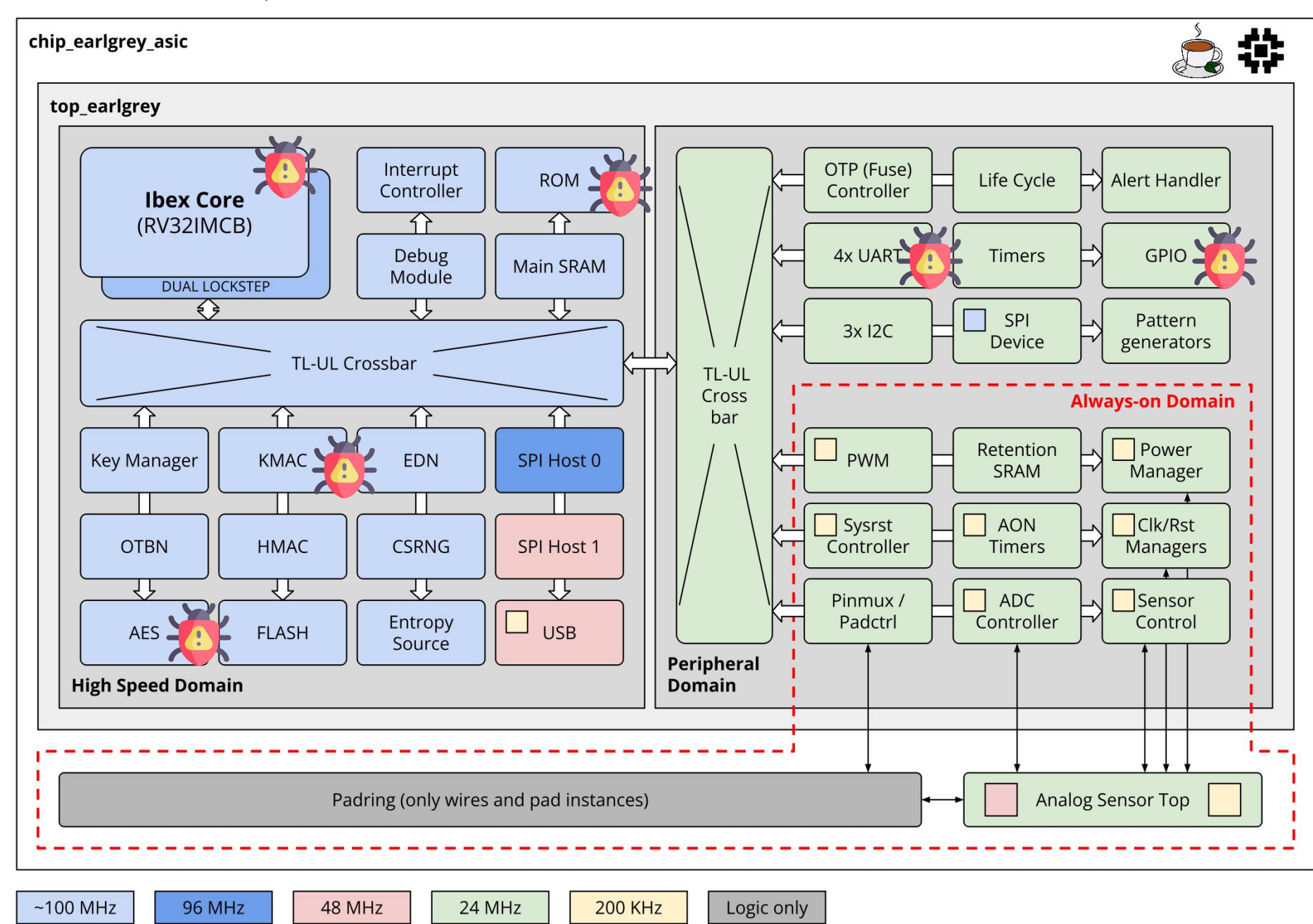
HACK@DATE 2025 RISC-V 硬件漏洞挖掘竞赛 冠军

参赛队伍: HASS Lab Team
 指导老师: 吴敬征 凌祥
 参赛队员: 吕浩 芮志清 王承杰 李志远
 联系方式: lyuhao23@mails.ucas.ac.cn

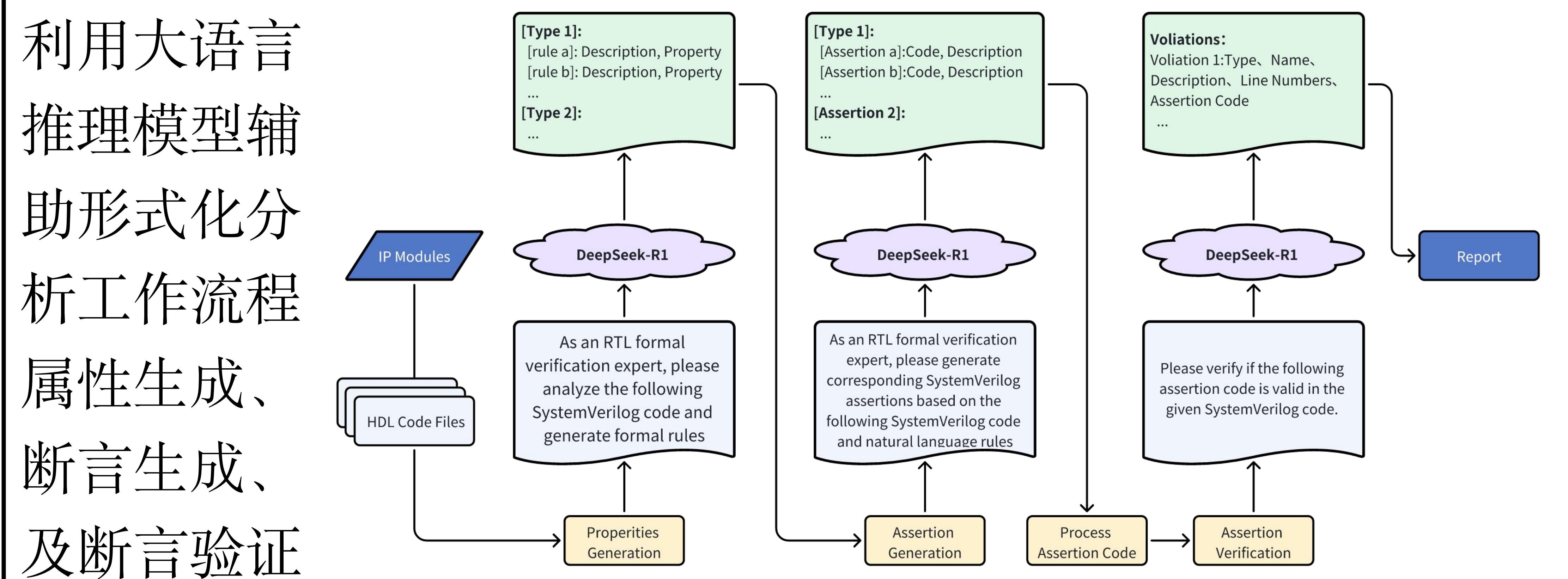
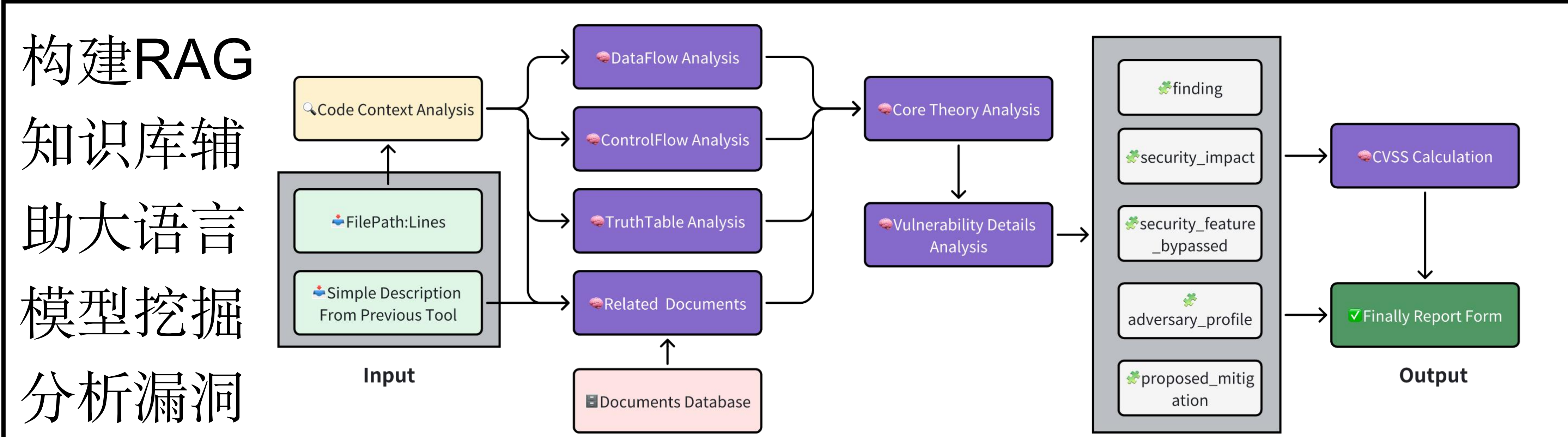


比赛介绍: HackTheSilicon 是硬件安全顶级赛事, 吸引来自学术界和工业界专家挖掘片上系统 (SoC) 逻辑实现中的漏洞, 由英特尔与达姆施塔特理工大学及得克萨斯 A&M 大学联合支持今年春季, HackTheSilicon团队在电子设计自动化领域顶级会议 DATE 2025期间组织比赛, 吸引来自中国、美国、英国、印度等国家和地区的27支战队、82名安全领域研究人员参与

比赛规则: 比赛分为初赛与决赛两个阶段, 参赛选手需在有限时间内挖掘出隐藏在开源 RISC-V SoC OpenTitan 多个 IP 中的漏洞, 分析并构建漏洞利用程序



技术路线: 使用 RAG 检测漏洞及大语言模型辅助形式化分析



在初赛和决赛共提交 **43** 个漏洞并成功构建 **21** 个漏洞利用程序
 最终 HASS Lab 战队以 **985** 分的绝对优势斩获总冠军
 打破该赛事历年得分记录!



This paper is supported by
Open Source Map