

## 船舶工业仿真软件源代码成分分析工具-技术要求

该工具以面向船舶工业软件为主要场景，交付物产品需要适配船舶工业软件的应用场景。

序号	货物（服务）名称	数量	单位	性能参数及技术指标（服务要求）
1	精细化代码成分拆解	1	套	多层依赖穿透：自动解析仿真软件的完整调用链，逐层剥离至底层基础库与中间件，清晰呈现“主程序—外购模块—开源组件—系统 API”的层级关系； 组件指纹画像：为每个代码片段生成唯一标识符（Hash 值+元数据），精准定位来源（商用/开源/自研）、版本号及修改记录； 跨语言兼容：支持 C/C++、Fortran、MATLAB 等工业仿真主流语言，适配 ANSYS、COMSOL 等商业软件二次开发场景。
2	供应链安全风险扫描	1	套	已知漏洞库匹配：实时比对 NVD、CVE、OSV 等漏洞数据库，标记存在高危漏洞的组件版本（如老旧 OpenSSL、Log4j 变种）； 许可证合规审查：自动识别 GPL、AGPL 等传染性许可证，预警商业授权超范围使用风险，避免法律纠纷； 后门/恶意代码检测：通过特征码匹配与行为分析，揪出隐蔽的远控指令、数据回传等恶意代码片段。
3	自主可控评估与替代	1	套	国产化适配度分析：量化评估代码对国产操作系统(麒麟、统信)、芯片架构(鲲鹏、龙芯)的兼容性，定位需改造的关键模块； 替换成本估算：针对高风险/不可信组件，推荐国内同类开源或商业方案，并提供重构工作量预估模型； 知识图谱可视化：以拓扑图展示代码依赖关系，高亮显示“卡脖子”环节，辅助制定去风险化路线图。
4	离线模式	1	套	支持本地漏洞库配置，代码不出内网即可完成扫描，适配涉密场景
5	二进制特征识别	1	套	二进制特征识别:无依赖配置文件场景下，通过组件特征码、文件哈希(MD5)、包名解析等方式，精准识别二进制包(如 JAR、WAR)中的组件