SOLUTIONS TESTING 泽众软件

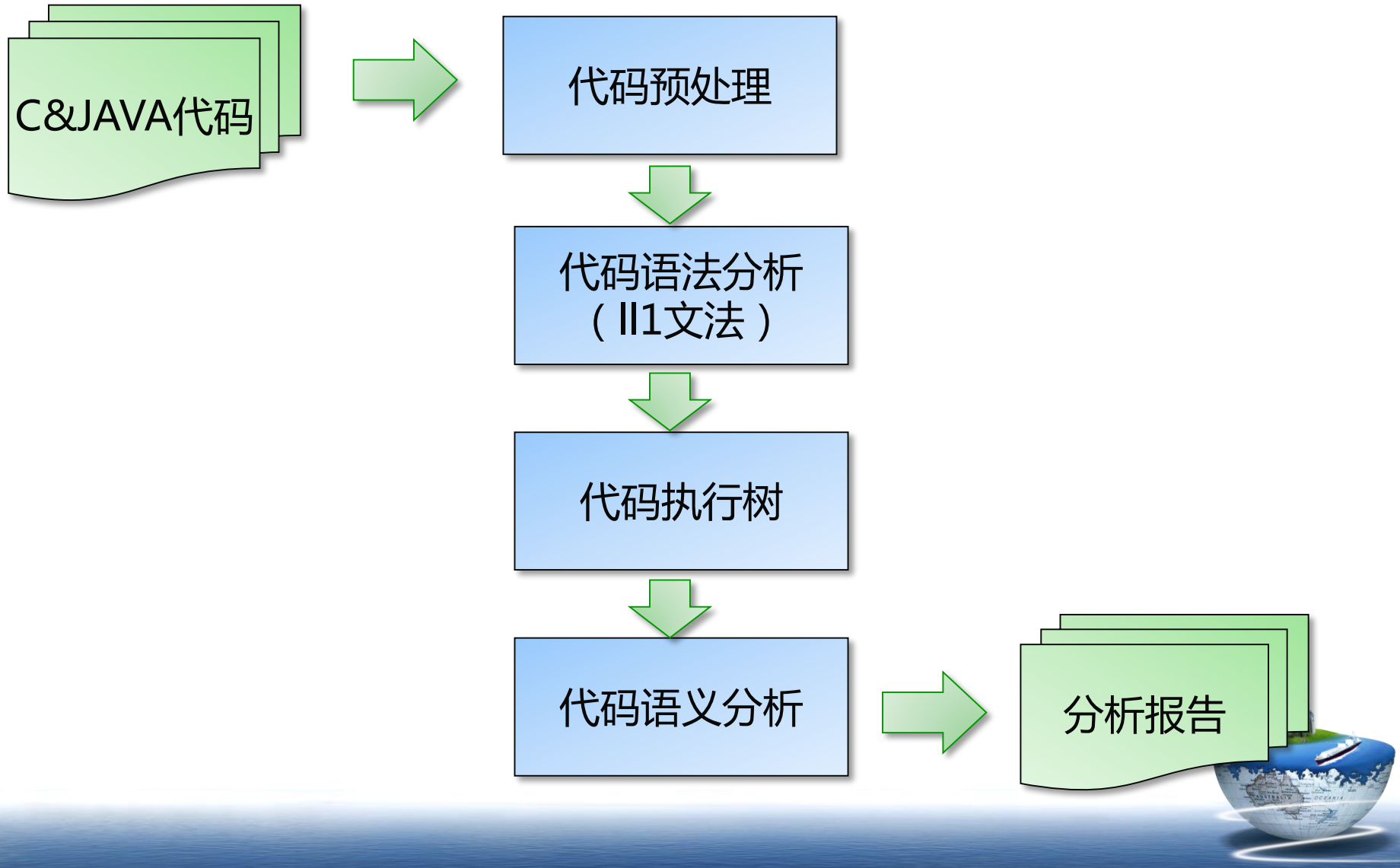
CodeAnalyzer(CA)静态代码分析产品介绍

——国内一流的白盒测试专家

课程目标

- 掌握CA基本的使用
- 通过一个实例的项目执行掌握如何进行代码扫描

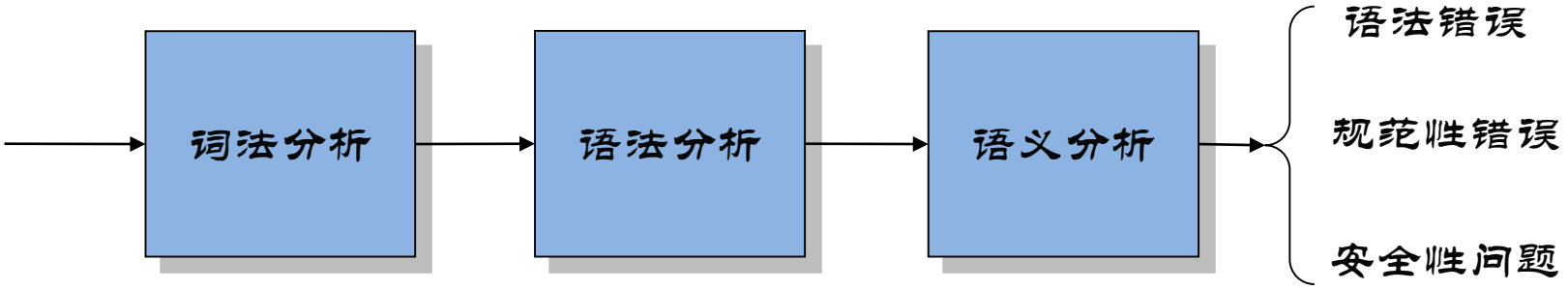
代码分析流程



代码分析方法

- 词法分析阶段和语法分析阶段是连续的两个处理过程，CA通过词法分析识别到源代码中的语法元素，通过语法分析验证源代码语法的正确性（每一个语法元素必须满足一定的文法规则，例如：
  - 编程语言中常见的循环语句：

for (init_part; condition; increment) statement



安全规则支持

- 代码规范检查
  - 支持500条内建代码规范
  - 支持用户自定义代码规范，可定制化的代码规范检查机制
- 代码安全检查
  - 内存泄露
  - 未访问变量声明
  - 无限循环
  - 其它代码安全隐患检测

支持的部分代码规范

- 下表罗列出CA软件支持的部分语法规则：

章节名称	规则定义	规则
命名规则		
	命名原则	标识符应当直观且可以拼读
		标识符的长度应当符合“min-length && max-information”原则
		命名规则尽量与所采用的操作系统或开发工具的风格保持一致
应用程序的命名		“系统简称”+模块名称
子模块的命名		每个子模块的名字应该由描述模块功能的1-3以单词组成。每个单词的首字母应大写
变量的命名		可以用多个英文单词拼写而成，每个英文单词的首字母要大写，其中英文单词有缩写的可用缩写；
		变量的前缀表示该变量的类型
		对于作用域跨越10行以上的变量名称不能少于4个字符

代码安全检查

- 代码安全检查是通过对代码进行语义分析，检查出代码中出现的安全隐患。

与其他系统集成

- 利用CA提供的用户接口API可以很方便地将CA集成到审计平台中，通过输出配置，将CA分析的结果数据保存到数据库表中
- 在测试体系中，可以使用CA评估开发工程师的工作量与工作质量，即“代码审计”