1 分析工具

1.1 静态分析

工业界：Converity，Foritify
学术界：CBMC,Frama-C
价格昂贵，运行快，覆盖面广

1.2 动态分析

工业界：Peach(测试协议)，Tsanitizer
学术界：Calfuzzer，Maple
隐私风险，代码泄露的可能，不完备，比如死锁、原子性违反等

1.3 代码生成

工业界：Simulink，SCADE
学术界：Ptolemy，Metro-Polis
技术封闭，无法有针对性优化

2 可信构造

图形化建模→图形化仿真→验证转换→代码生成

2.1 正向建模的问题

如何建模
建模后如何分析
代码生成器正确性

2.2 逆向建模

找到模型的缺陷

符号执行

3 CPS的问题

Reliability
Safety

4 Model-Driven Design

关键步骤：设计正确，实现和设计一致
需要工具：从需求抽取Model，证明Model正确，implementation正确的度量

Read Time Protocol：Connection，Transfer，Disconnection

4.1 Ongoing Work

Dynamic analysis of Embedded Code()
Dynamic analysis of CPS()
Dynamic analysus of Model(Concurrency Bug Detection)