**PASAN: Detecting Peripheral Access Concurrency Bugs**

**within Bare-Metal Embedded Applications**

**Contribution：**

1、定义了正确的保护以同时考虑MMIO地址范围和外设的内部状态机。

2、设计并实现了用于检测嵌入式系统中外设访问的潜在并发错误的静态分析工具。

3、通过评估实际嵌入式平台，在三个不同的平台上发现总共17个并发错误。

**Motivation:**

目前大多数检测并发错误的方法没有考虑总线和外围级别内部状态机中的竞争条件导致的并发问题。

**Key Idea：**

利用地址范围感知策略和事务感知策略进行静态分析检测

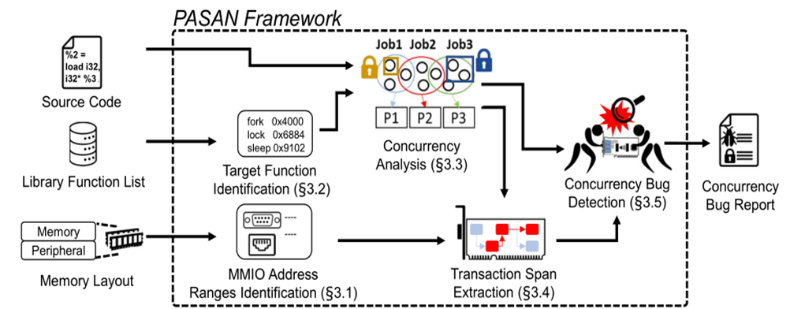
**Challenges:**

1、如何自动查找外设的MMIO地址范围？

2、如何自动查找外设的事务范围？

3、如何使用MMIO地址和事务范围来自动查找错误？

**Design:**



* **MMIO Address Ranges Identification**

利用主机的内存布局文档，包括系统视图描述 (SVD) 文件或特定于主机的开发工具库。

* **Target Function Identification**

通过分析目标LLVM位码，PASAN识别与分析并发可执行函数相关的函数（例如，多进程、多线程、锁定和中断管理函数）。如果从源文件中没有找到相关函数，查找与中断相关的体系结构特定的汇编指令。

* **Concurrency Analysis**

PASAN识别可执行进程、线程和中断处理程序；分析它们以识别可并发执行的指令；执行锁集分析以识别被“锁定”以防止并发访问的指令。

* **Transaction Span Extraction**

PASAN通过开发一组跨度提取启发式方法来识别所有事务跨度。先通过跟踪store和load指令来查找外设访问指令，接着利用指令列表及其访问的MMIO地址范围来确定一个事务范围，与此同时需要处理指令的调用。

* **Concurrency Bug Detection**

PASAN验证确定的事务跨度是否被现有锁对象正确覆盖。并通过自动检查MMIO地址是否可以在没有适当的锁跨度的情况下并发访问，实现了并发错误的检测。