**[平头哥杯](http://univ.ciciec.com/nd.jsp?id=559" \l "_jcp=1)**

**一、杯赛题目：基于无剑100开源SoC平台构建双核TEE安全系统**

**二、参赛组别：A组、B组**

**三、赛题任务：**

随着物联网(IOT)的高速发展，信息安全问题突显，可信执行环境（Trusted Execution Environment，TEE）是保障信息安全的有效手段，因此在RISC-V处理器上构建TEE的安全能力是眼下比较热门的话题。

本赛题旨在利用平头哥开源的RISC-V处理器（E902）设计一个支持TEE的最小系统，为RISC-V处理器构建TEE的安全原型。双核TEE安全架构中，其中一个E902核心用作安全核，运行安全世界程序，另一个E902核心用作非安全核，运行非安全世界程序。通过双核方案实现CPU在物理上的隔离，并且需要设计一个IOPMP(物理地址访问防火墙)，来确保非安全世界的master设备(包括非安全CPU和非安全外设)无法访问安全世界的资源，包括内存和MMIO。E902安全核和非安全核之间的通信需要用到mailbox设备，安全世界的mailbox属于安全设备，非安全世界的mailbox属于非安全设备。系统需要实现安全启动方案，安全CPU核心需要对软件镜像进行合法性校验，在完成软件镜像的合法性校验以及安全配置之后再启动非安全CPU核心的运行。

**参考建议：**

在E902非安全核后面接一个地址访问防火墙，比如IOPMP，用于约束非安全E902核对内存、MMIO的访问。CPU以外的master设备同样需要通过IOPMP来限制其访问。

**参考平台：**

SoC平台可以参考平头哥无剑100开源SoC平台：

1. 平头哥无剑100 SoC 平台简介：<https://occ.t-head.cn/wujian100?id=4082555169550700544>

2. 平头哥无剑100 开源SoC平台软硬件源码：<https://github.com/T-head-Semi/wujian100_open>

3. 对FPGA的型号并无要求，开发者可以自由选择FPGA开发平台，如Xilinx FPGA等。

**四、提交内容：**

1. 作品展示，包括技术创新、项目内容和后续工作

2. 设计报告：

(1) 项目背景

(2) 系统架构和安全方案，包含处理器、内存、I/O和调试的隔离方案，安全启动流程，以及关键模块的描述

(3) 功能仿真、FPGA测试结果

(4) 总结

(5) 参考文献和团队介绍

3. 设计代码：

(1) SoC平台代码

(2) 安全启动代码

(3) TEE/REE软件栈

**五、评分标准：**

|  |  |  |
| --- | --- | --- |
| **评分级别** | **功能实现** | **得分** |
| 基础任务 | SoC至少包括基础双核E902+存储（SRAM）+IO(2个串口) | 30 |
| 每个E902核分别运行独立的软件程序，并从串口输出打印信息 | 20 |
| SoC实现BootROM，并实现安全启动机制，比如: BootROM->TEE Code ->REE Code | 20 |
| 中级任务 | BootROM实现从Flash加载程序并启动 | 20 |
| SoC实现Mailbox，双核E902通过Mailbox建立核间通信 | 20 |
| 高级任务 | SoC实现IOPMP访问防火墙，通过IOPMP来控制E902非安全核的对内存(SRAM)、MMIO(如串口)的访问权限 | 20 |
| 设计报告 | 设计报告应详细阐述技术方案，尤其需要突出如何实现中、高级任务的技术要点，报告应结构清晰、逻辑流畅、详略得当。 | 10 |
| 技术路线 | 在实现中、高级任务时，应与现有的常规技术路线进行对比。如果在技术路线上有成功的改进或突破，可以根据技术路线的先进性判别得分。 | 10 |
| 总分 |  | 150 |

评分表补充说明：

1. 所有任务，功能每实现一项，即可得到该项所有分数

2. 如果未完全实现某项功能，根据技术报告的内容酌情给分

**六、注意事项：**

1. 参加企业命题杯赛的作品，杯赛出题企业有权在同等条件下优先购买参加本企业杯赛及单项奖获奖团队作品的知识产权。

2. 大赛组委会和杯赛企业对参赛作品提交的材料拥有使用权和展示权。

3. 参赛项目可以参考现有公开发表的文献和论文内容，但应当在技术论文和答辩PPT中注明来源，且不能将参考的内容作为自己作品的创新部分。