芯来科技
NUCLEI

基于轻量级RPC的RISC-V调试方案

万瑞罡 06·2022

目录

芯来科技
NUCLEI

- 总体介绍
- 现有调试方案存在的不足
- 我们所提出的解决方案
- 性能对比

总体介绍

现代处理器/微控制器中一般拥有调试模块，可承担如下功能：

- 存储器编程(Programming)
- 软件调试(Interactive Debug)、跟踪(Trace)
- 性能分析(Performance Analysis)
- 量产编程与测试(Massive Production)

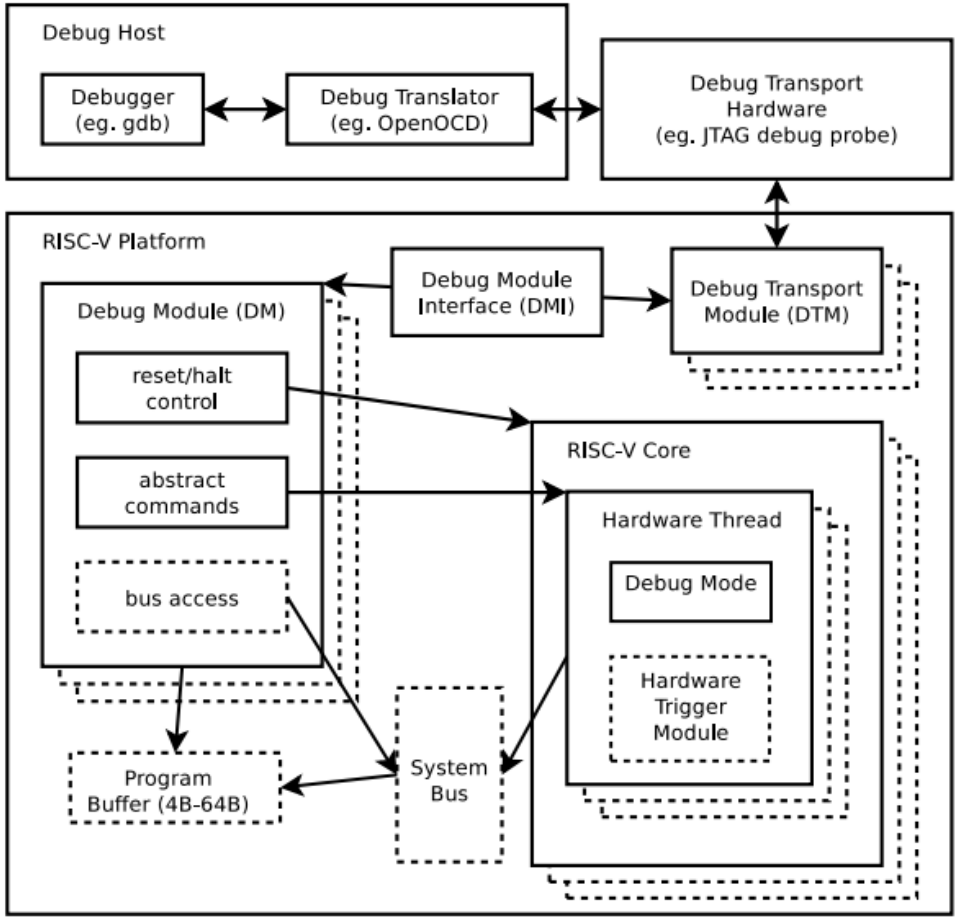
但仅有调试模块，是不够的。必须有一套配套的软硬件工具，
才能够在实际开发、生产环境上实现如上所述的功能。

这套软硬件方案即为调试方案。

总体介绍

芯来科技
NUCLEI

完整的RISC-V调试组成框图



造成性能问题的原因

RISC-V 调试模块操作流程：

（1）填充DMI寄存器的DM地址、数据与操作码；
（2）等待DTM模块中DTMCS（DTM Control and Status）寄存器中要求的Run-Test-Idle周期；
（3）回读DMI寄存器，检查状态位。若DMI忙，则重复第2步，等待操作结束为止。若DMI错误，则进入错误处理流程。

其中（3）步需要主机回读状态，主机<->调试模块间的延迟就成为了吞吐量受限的瓶颈，直接影响访存带宽，降低调试效率。

现有调试方案存在的不足

芯来科技
NUCLEI

开源方案

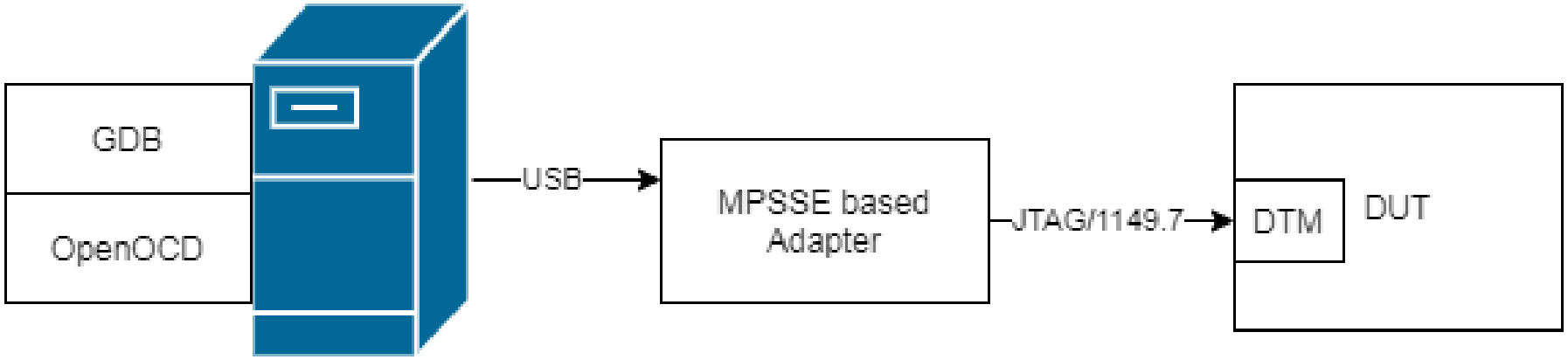
- OpenOCD
- RV-Link

商业方案

- SEGGER J-Link
- Lauterbach TRACE32

OpenOCD调试系统应用框图

芯来科技
NUCLEI



OpenOCD所存在的一些问题

芯来科技
NUCLEI

（1） OpenOCD 本身框架中存在的问题：

1. 对系统信号(signal)响应有问题
2. 存在内存泄漏、句柄泄漏、非法访问等问题
3. 抽象层次不明确，导致同样功能被不同目标（target）驱动重复实现
4. 为资源较为宽裕、运行分时操作系统的设备编写，如引入 Jimtcl 等库，难于移植到硬件资源较少的硬件平台上（如离线编程器）
5. 没有统一的二进制插件接口，也没有稳定的内部API，导致二次开发的插件必须跟随主线升级

其中第一与第二点问题会不定时的引发OpenOCD崩溃，在调试时导致用户使用体验较差。

（2） OpenOCD RISC-V 目标驱动中存在的问题：

1. 使用同步I/O机制操作调试模块，吞吐量受调试接口<->主机之间的往返延迟制约
2. （截至2022/04）仅实现了对基于JTAG的调试传输模块（DTM）的支持，对新协议支持需要再做改动
3. （截至2022/04） Semihosting 支持暂时还不完善

RV-Link的优势与劣势

优势：

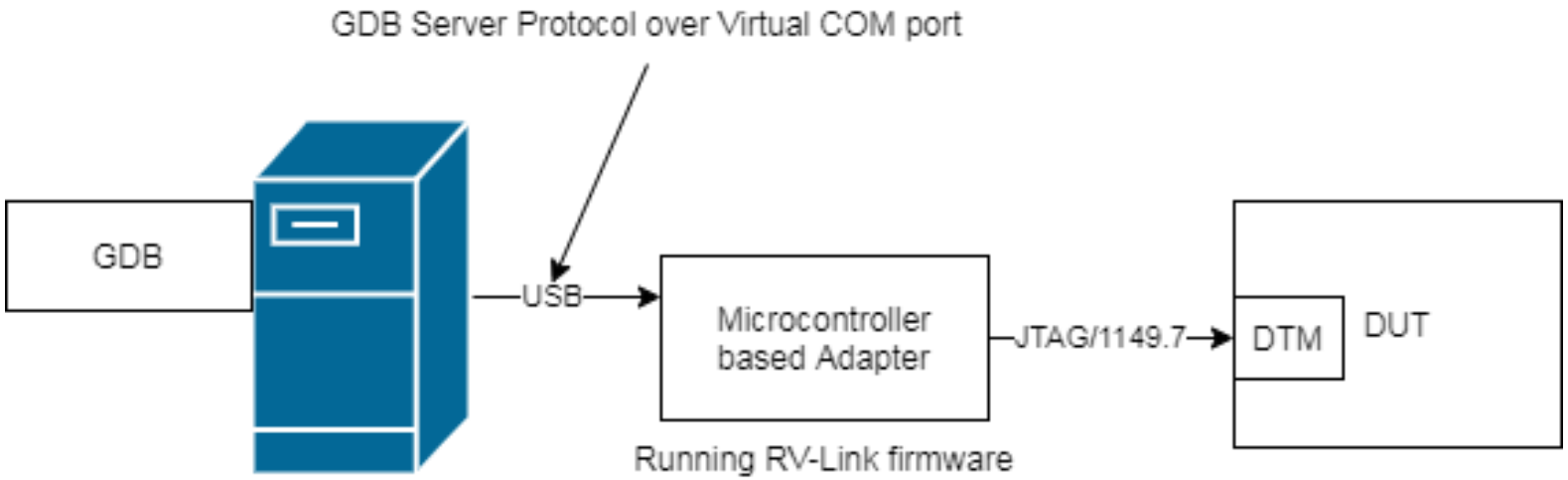
1. 所有I/O操作均被卸载到调试适配器上，往返延迟低，性能好
2. 使用标准GDB Server协议与调试器互操作，兼容性好
3. 代码没有对特定操作系统的依赖，能够裸机运行，适用场景较多

劣势：

1. 调试适配器本身资源有限，难于存储不同的设备支持表、外设支持驱动等必要的信息，使得支持设备的数量较少
2. 使用GDB Server协议与主机通讯，难以承载其他的调试需求，如裸JTAG通讯等
3. 暂无完善的固件升级方案，难于解决使用固件升级的方式对系统增加功能，或是修复问题

RV-Link调试系统应用框图

芯来科技
NUCLEI



芯来科技
NUCLEI

社区需要一个全新的解决方案应对这些问题

调试系统设计需求

芯来科技
NUCLEI

- 需要解决上述方案的性能问题
- 需要对各个功能组件解耦，杜绝重复实现功能的叠床架屋
- 架构应设计的灵活而有扩展性
- 需具备跨平台特性，主机操作系统至少支持Linux与Windows系统
- 能至少在主机上为第三方提供稳定的二进制插件接口
- 能支持多种调试传输模块（DTM）协议，不局限于JTAG

Confidential ©2022 Nuclei. All Rights Reserved.

Morpheus 调试系统设计理念

芯来科技
NUCLEI

在缓存设置合理的情况下，异步传输的吞吐率并不会因为延迟增加而产生明显下降。同步传输由于需要在每一步状态改变之后等待对方设备响应，实际吞吐率和全链路的延迟呈现负相关。

因此，为了解决系统的传输瓶颈，应当将同步传输局限于调试适配器与待测系统之间，而在主机-调试适配器间使用异步传输，以求最大化的降低延迟。

将所有功能均卸载到调试适配器上，仅对主机暴露最终调试接口的设计范式，也能够满足上述要求。但调试适配器本身处理性能较主机弱、存储容量较主机小。这些缺点限制了它的扩展性与它能够达到的性能上限。

Confidential ©2022 Nuclei. All Rights Reserved.

Morpheus 调试系统设计理念

芯来科技
NUCLEI

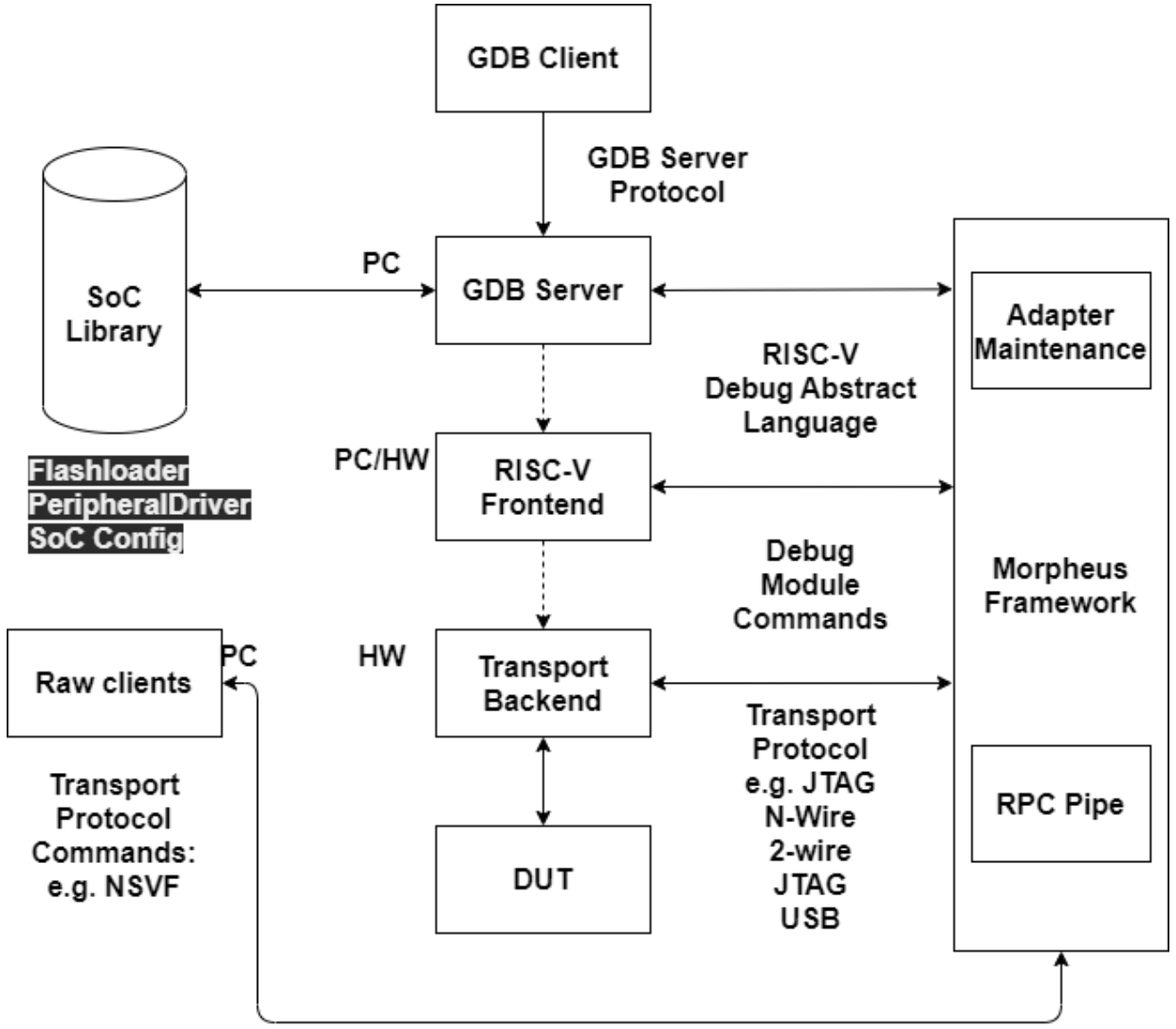
因此，我们需要在全部将功能卸载到调试适配器上，与所有功能均在主机上两种方案之间取得折中。此外，我们还需要所有必要的调试功能有比较好的跨平台性，这样能够将所有的功能都放置到主机端，便于使用仿真/验证环境，且能兼容早期基于FTDI MPSSE的调试器。

为了平衡开发效率与运行效率，我们最终使用RPC的方式，使得各个被分拆出的功能模块间能够互相调用，且开发体验类似于在单机上开发程序。

Confidential ©2022 Nuclei. All Rights Reserved.

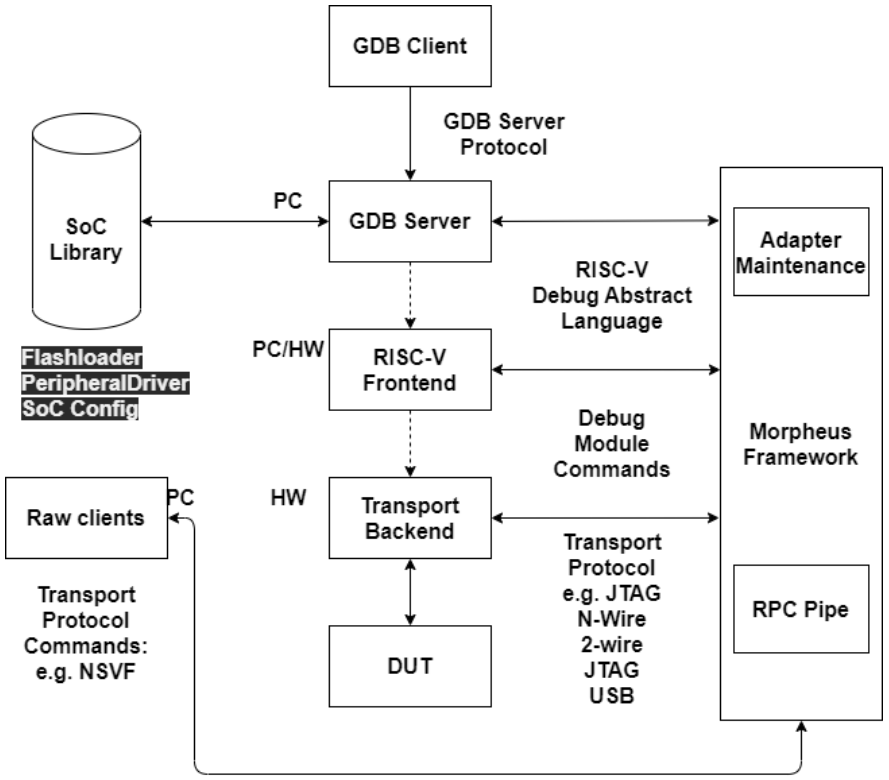
Morpheus 调试系统框图

芯来科技
NUCLEI



Morpheus 调试系统框图

芯来科技 NUCLEI



· SoC Library：提供目标系统的配置信息、驱动程序等必要信息。

· GDB Server：直接提供对GDB或其他GDB 协议客户端的调试服务功能，产生合适的调试抽象命令

· RISC-V Frontend：根据待测系统的调试协议版本，将调试抽象命令转换成相应的DM控制命令序列。

· Transport Backend：将对应的DM控制命令序列转换成DTM所需要的时序，并连接DTM，提供调试的物理通路。

· Morpheus Framework：提供各个组件之间的互操作与异步I/O接口的定义和参考实现。实现轻量化的RPC协议，完成适配器/主机软件版本同步并可以提供裸JTAG等编程接口，方便将来用单调试口承载多种调试业务，如Xilinx PL JTAG。

Confidential ©2022 Nuclei. All Rights Reserved.

各组件的硬件资源限制

芯来科技
NUCLEI

- 非主要在PC端执行的组件，以4-8KB SRAM、32KB Flash的硬件规格，无动态内存管理，作为其开发的资源限制。

- PC端执行的组件，以一般PC的资源（单核 512M内存）作为其资源限制。

Confidential ©2022 Nuclei. All Rights Reserved.

适配器硬件选型

芯来科技
NUCLEI

- 初代交互式调试硬件基于兆易创新GD32或安路ELF2 FPSoC。

使用外置74逻辑门电路实现双向电平转换。降低硬件成本便于铺开。

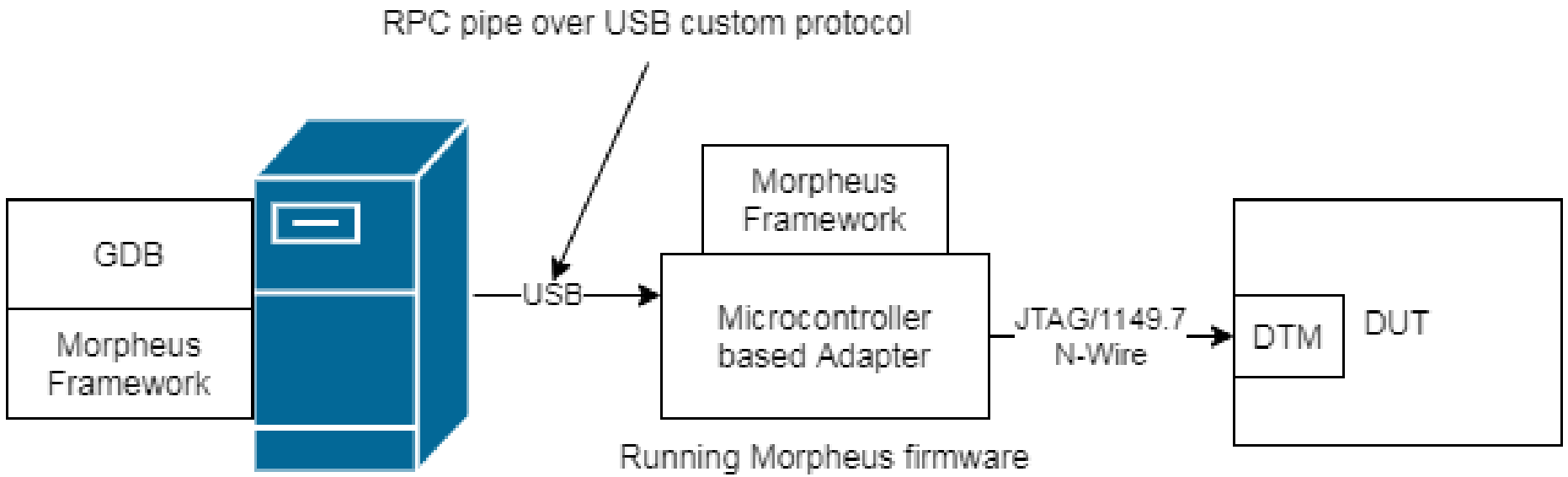
- Trace调试硬件基于USB3.0接口芯片与FPGA平台开发。

- 初代离线编程器同样基于交互式调试硬件设计，仅加入屏幕、

SDIO接口和PASS-FAIL接口，用于连接程序存储器、ATE设备等。

Confidential ©2022 Nuclei. All Rights Reserved.

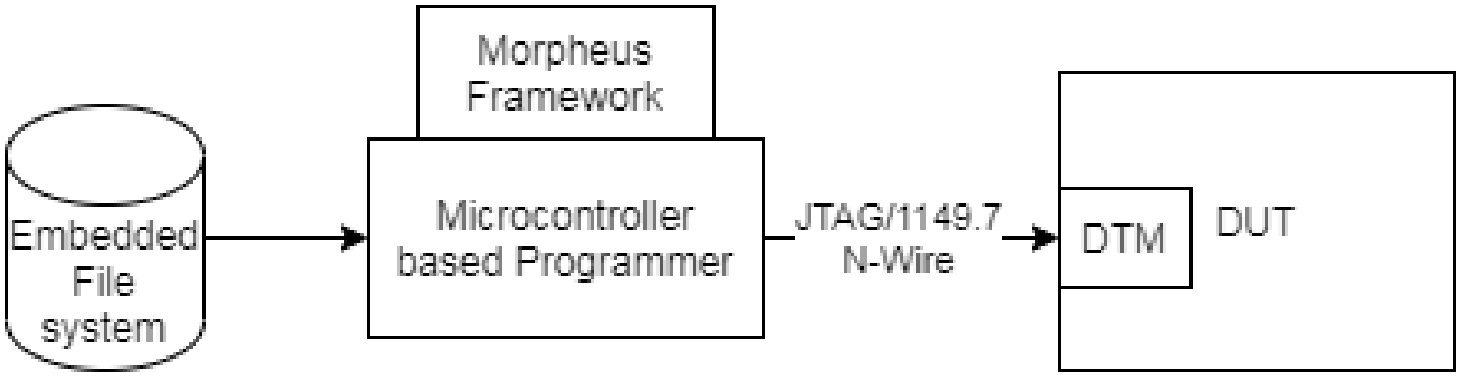
Morpheus 调试系统应用框图（调试）



Confidential ©2022 Nuclei. All Rights Reserved.

Morpheus 调试系统应用框图（离线编程）

芯来科技
NUCLEI



Confidential ©2022 Nuclei. All Rights Reserved.

轻量级RPC的实现

芯来科技 NUCLEI

基于简单的TLV（Type-Label-Value）帧格式，运行在保证按序可靠交付的帧式管道上。

· 可基于USB Custom/CDC协议的Bulk传输实现
· 可基于TCP/IP协议实现
· 可基于简单的共享内存块实现（运行在同一进程中）
· 调用实体 Id 在编译期生成，使用 SHA 算法对函数名进行 Hash 后生成前 16 位，后 8 位按重名顺序生成，节约运行资源。

表 1　RPC 协议帧格式

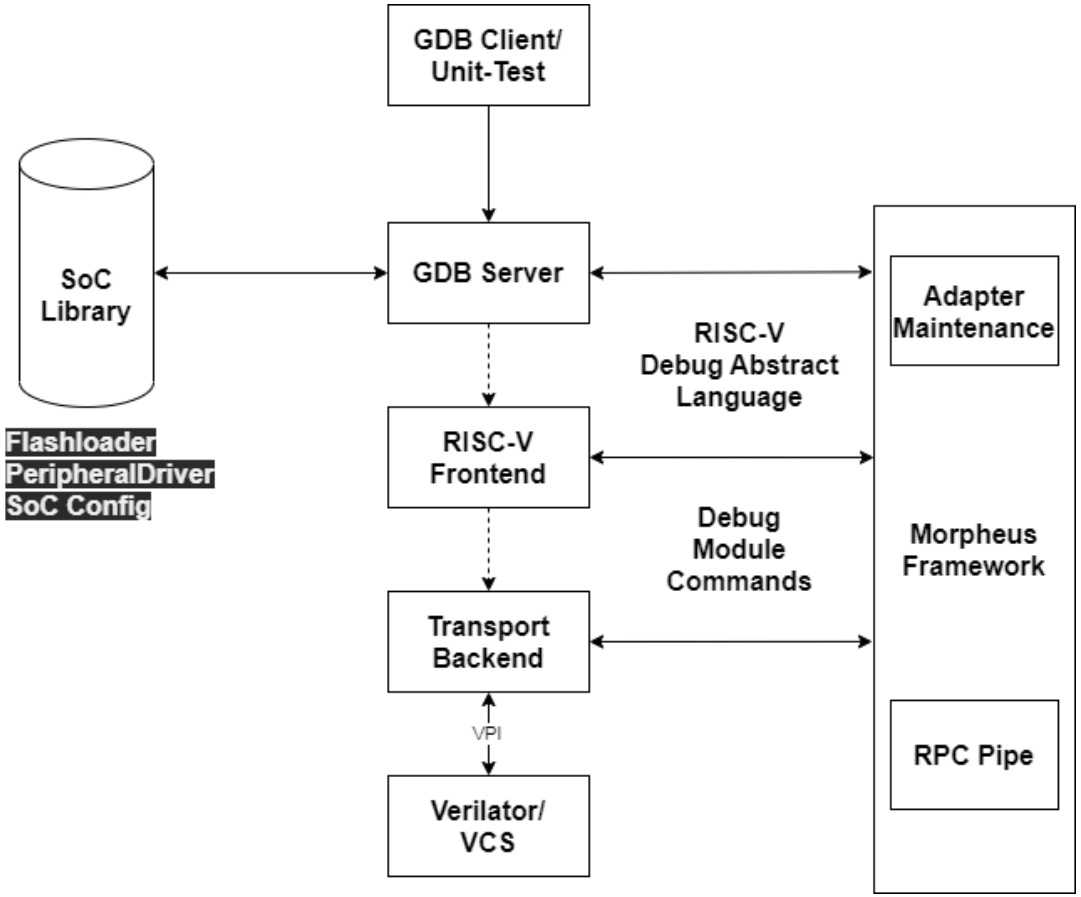
序号	名称	长度	备注
1	帧类型	8-bit	指示帧类型
2	调用实体 Id	24-bit	RPC 函数编号
3	载荷 1	n-bit	载荷 1（可选）
n	载荷 n	n-bit	载荷 n（可选）

表 2　载荷格式

序号	名称	长度	备注
1	载荷 Id	8-bit	指示载荷名称
2	载荷类型 Type	8-bit	指示载荷类型
3	载荷长度 Len	16-bit	载荷长度（可选）
4	载荷数据 Value	n-byte	载荷数据

VPI 验证环境的实现

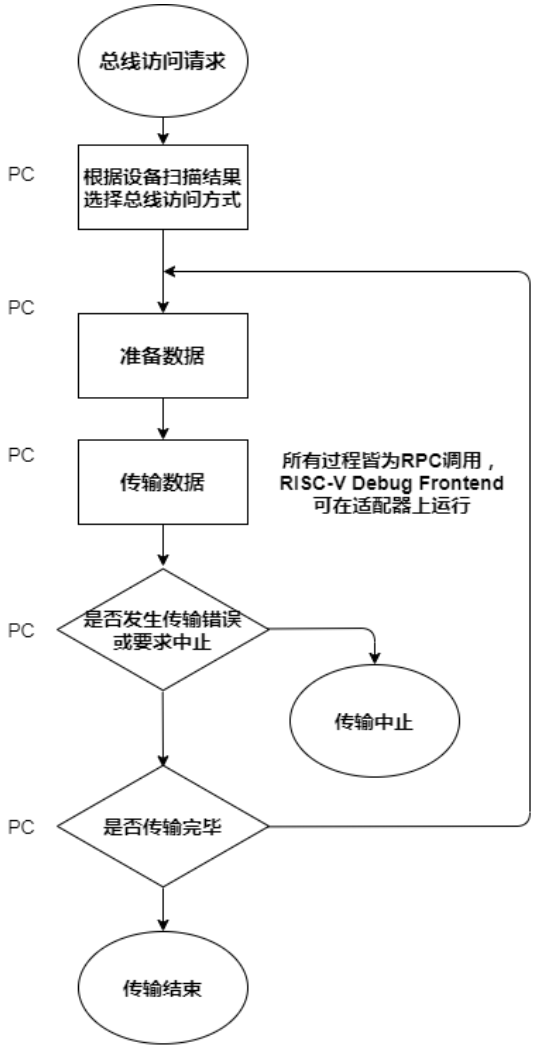
芯来科技
NUCLEI



在传输后端实现VPI接口，可与仿真环境接口，产生JTAG时序或直接与目标系统的Debug Module Bus接口。实现仅需纯软件实现下与硬件仿真环境的对接及相互验证。

总线访问流程的性能优化

芯来科技 NUCLEI



处理总线访问请求流程为：

由位于主机的GDB Server负责接收或提供数据，以RPC的方式对位于调试适配器固件中的RISC-V Frontend组件进行调用，RISC-V Frontend根据命令和总线访问方式，进行可选的虚拟地址-物理地址转换，产生对应的DM访问序列，由之前已选择好的DTM传输接口所对应的后端发出。每一次主机会向调试适配器提供或要求最多为调试适配器报告的支持的缓冲区大小的数据，而后主机等待传输完成。

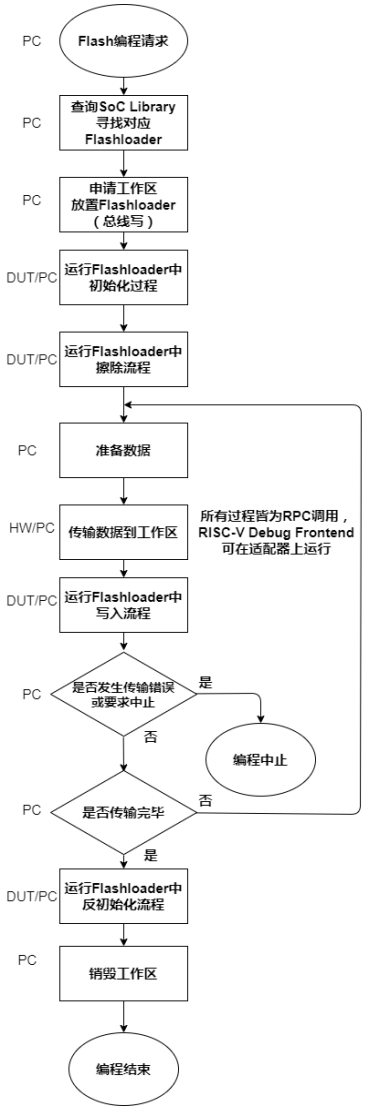
由于RISC-V Frontend组件与Transport Backend组件均可运行在调试适配器上，且调试适配器使用微控制器实现，故比主机直接控制的方式能提供较低的输入输出延迟，由此达到提高传输效率，降低数据传输时间的目的。

其流程如左图所示，其中调试适配器流程为：等待RPC调用->传输数据->调用RISC-V Frontend->处理回复。

Confidential ©2022 Nuclei. All Rights Reserved.

Flash编程流程的性能优化

芯来科技 NUCLEI



由于主机对待测系统通信延迟高，Morpheus调试协议栈为提高效率和简化设计，不支持类似OpenOCD将Flash驱动直接实现在主机侧的Flash驱动方案，强制使用基于Flashloader的Flash驱动方案。

在调试客户端请求Flash编程后，GDB Server将根据系统配置，在待测系统上寻找一块合适的允许执行的内存块，申请足够大小的内存，该内存块被称为工作区。申请到工作区后，将工作区分为程序区与数据缓冲区，将Flashloader写入程序区。

GDB Server再根据Flashloader与已约定好的ABI与Label，运行Flashloader的初始化过程与擦除过程，在确认初始化和擦除过程成功完成后，进入编程循环：

1. GDB Server将对申请到的数据缓冲区写入部分数据。
2. 运行Flashloader的写入流程，不断重复编程循环。

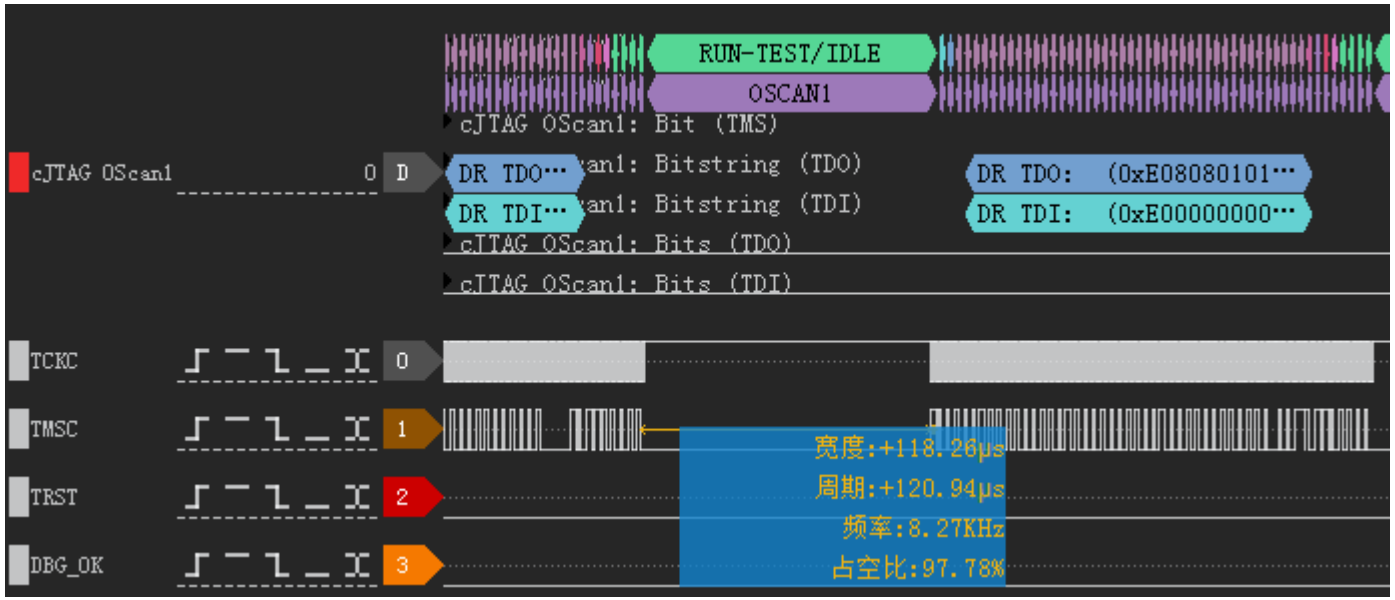
直到所有数据均被正确编程到Flash中。

在Flash编程完毕后，GDB Server将运行Flashloader的反初始化流程，确保系统被复原。然后销毁工作区，完成整个编程流程。流程如左图所示。

Confidential ©2022 Nuclei. All Rights Reserved.

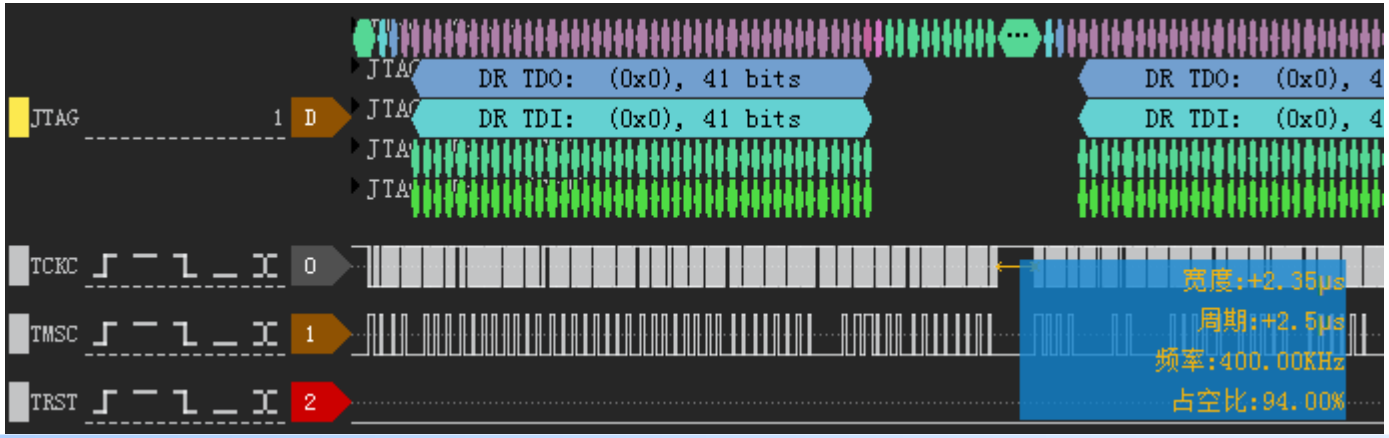
性能对比

芯来科技 NUCLEI



左上图为OpenOCD使用IEEE 1149.7协议操作芯来科技 N307 处理器的 DTM 波形，可见每一次请求间存在 120μs 左右的延迟。此时对RAM的写入速率约57KB/s对Flash的写入速率约9KB/s。

TCK频率均为4MHz。



左下图为Morpheus使用IEEE 1149.7协议操作芯来科技 N307 处理器 DTM 波形，可见每一次请求间的延迟已被降低到 2.5μs 左右，延迟缩短到原来的1/48。此时对RAM的写入速率约141KB/s，对Flash的编程速率约16KB/s。

Confidential ©2022 Nuclei. All Rights Reserved.

总结

芯来科技
NUCLEI

- 将对延迟敏感的操作卸载到调试适配器上，提高吞吐量
- 解耦多个功能组件，提高架构扩展性
- 支持多种调试传输模块（DTM）协议

Confidential ©2022 Nuclei. All Rights Reserved.

未来将实现的功能

(1) 稳定的GDB Server
(2) SBA接口所必要的虚拟地址<->物理地址转换
(3) 对 SMP 系统的支持
(4) 完整的离线编程器实现框架
(5) Semihosting 与 Flash 软断点
(6) 完成二次开发接口的设计

芯来科技
NUCLEI

请各位提问

芯来科技
NUCLEI

谢谢！