

## 32 位 ARM 嵌入式处理器的调试技术

文章作者：李 剑 赵鹏程 汤建彬

**摘 要：**针对 32 位 ARM 处理器开发过程中调试技术的研究，分析了目前比较流行的基于 JTAG 的实时调试技术，介绍了正在发展的嵌入式调试标准，并展望期趋势。

**关键词：**嵌入式 调试 处理器 JTAG Nexus ARM

随着对高处理能力、实时多任务、网络通信、超低功耗需求的增长，传统 8 位机已远远满足不了新产品的要求，高端嵌入式处理器已经进入了国内开发人员的视野，并在国内得到了普遍的重视和应用。ARM 内核系列处理器是由英国 ARM 公司开发授权给其他芯片生产商进行生产的系统级芯片。目前在嵌入式 32 位处理器市场中已经达到 70% 的份额。笔者在对三星公司的 ARM7 芯片技术调试的过程中，对这些高端嵌入式系统的调试技术进行了总结。

传统的调试工具及方法存在过分依赖芯片引脚、不能在处理器高速运行下正常工作、占用系统资源且不能实时跟踪和硬件断点、价格过于昂贵等弊端。目前嵌入式高端处理器的使用渐趋普及。这些处理器常常运行在 100MHz，并且一些内部控制以及内部存储器的总线信号并不体现在外部引脚上。这种片上系统（System on Chip）、深度嵌入、软件复杂的发展趋势给传统的调试工具带来了极大的挑战，也给嵌入式处理器开发工程师的工作带来了不便，这就需要更先进的调试技术和工具进行配套。本文将详细介绍在 ARM 处理器中采用的几种片上调试技术（on-chip debugger）。这些片上调试技术通过在芯片的硬件逻辑中加入调试模块，从而能够降低成本，实现传统的在线仿真器和逻辑分析仪器的功能，并在一定的条件下实现实时跟踪和分析，进行软件代码的优化。

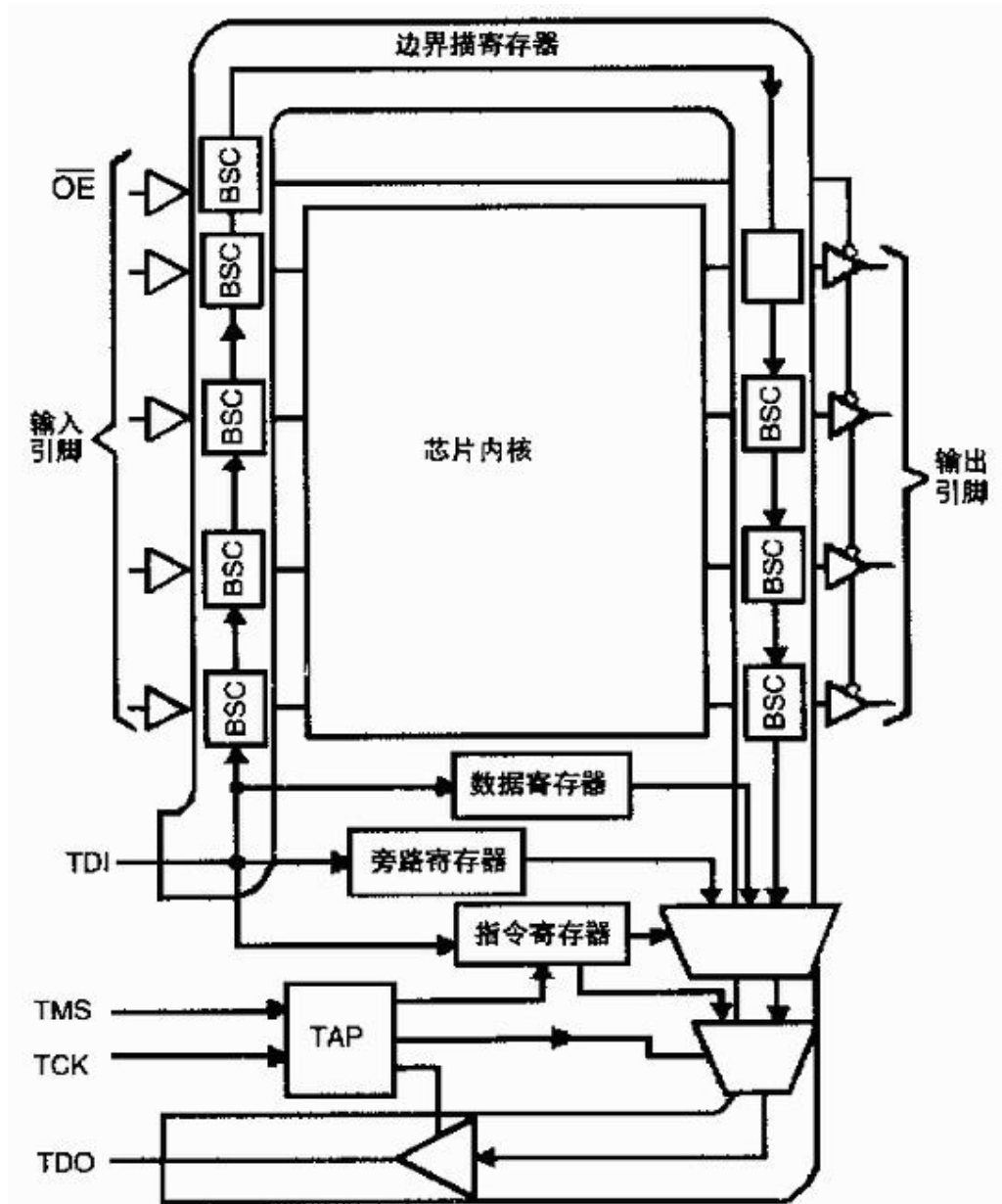


图 1 边界扫描体系结构

## 1 边界扫描技术 (JTAG)

边界扫描技术是为了满足当今深度嵌入式系统调试的需要而被 IEEE1149.1 标准所采纳，全称是标准测试访问接口与边界扫描结构 (Standard Test Access Port and Boundary Scan Architecture)。JTAG 遵循 1149.1 标准，是面向用户的测试接口，是 ARM 处理器调试的基础。本文提到的 ARM 的 E-TRACE 调试模式实际上是 JTAG 的增强版本，其它一些 32 位嵌入式处理器的调试方式也基本上遵循这个标准。这个用户接口一般由 4 个引脚组成：测试数据输入 (TDI)、测试数据输出 (TDO)、测试时钟 (TCK)、测试模式选择引脚 (TMS)，有的还加了一个异步测试复位引脚 (TRST)。其体系结构如图 1。

所谓边界扫描就是将芯片内部所有的引脚通过边界扫描单元（BSC）串接起来，从 JTAG 的 TDI 引入，TDO 引出。芯片内的边界扫描链由许多的 BSC 组成，通过这些扫描单元，可以实现许多在线仿真器的功能。根据 1149.1 的规定，芯片内的片上调试逻辑通常包括一个测试访问接口控制器（TAP）。它是一个 16 状态的有限状态机以及测试指令寄存器、数据寄存器、旁路寄存器和芯片标识寄存器等。在正常模式下，这些测试单元（BSC）是不可见的。一旦进入调试状态，调试指令和数据从 TDI 进入，沿着测试链通过测试单元送到芯片的各个引脚和测试寄存器中，通过不同的测试指令来完成不同的测试功能。包括用于测试外部电气连接和外围芯片功能的外部模式以及用于芯片内部功能测试（对芯片生产商）的内部模式，还可以访问和修改 CPU 寄存器和存储器，设置软件断点，单步执行，下载程序等。其优点如下：

- 可以通过边界扫描操作测试整个板的电气连接，特点为表面贴元件提供方便；
- 各个引脚信号的采样，并可强制引脚输出用以测试外围芯片；
- 可以软件下载、执行、调试和控制，为复杂的实时跟踪调试提供路径；
- 可以进行多内核和多处理器的板级和芯片级的调试，通过串接（如图 2），为芯片制造商提供芯片生产、测试的途径。

虽然 JTAG 调试不占用系统资源，能够调试没有外部总线的芯片，代价也非常小；但是由于 JTAG 是通过串口依次传递数据，速度比较慢，只能进行软件断点级别的调试，自身还不能完成实时跟踪和多种事件触发等复杂调试功能。因此便有了几种功能更为完善的增强版本。

## 2 ARM 芯片的实时调试方案（E-TRACE）

ARM 公司的内核芯片采用 E-TRACE 片上调试模式。它实际上是 JTAG 的升级版本，通过增强的辅助片上调试硬件来完成实时调试，解决了许多传统调试器难以解决的问题。

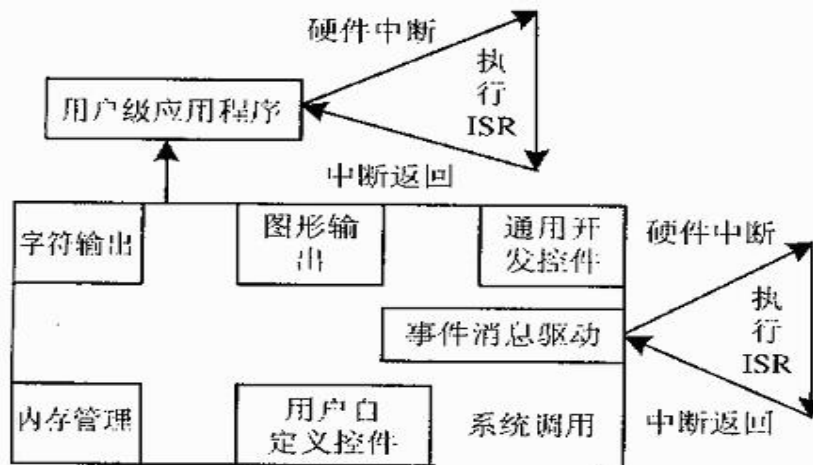


图 2 XGW 软件开发平台

图 2 对多内核和多处理器的调试

它的实时调试方案通过三种途径解决：

- EmbeddedICE 硬逻辑；
- 实时监控；
- 实时跟踪。

EmbeddedICE 逻辑单元存在于 ARM7TDMI、ARM9TDMI、ARM9E 和 ARM10 内核中。它枯 JTAG 口的基础上，增加了硬件断点寄存器、比较器，通过断点寄存器的值可以进行硬件断点的设置，不仅对地址还可以对数据、控制总线的信号进行复杂的触发控制设定，而不是单单在指令级别进行中断（如软中断），从而满足对特定事件的中断响应，极大的增加了灵活性，同时可以在 ROM 中设置断点和观察点，极大地方便调试。其示意如图 3。

实时监控则是进一步在 ARM9E 和 ARM10 中的改进。它改变 EmbeddedICE 在触发中断后时入调试模式状态而停止内核运行的弊端，进入一段非常小的中断监控程序中，得到所需要的信息后迅速把控制权转让给先前的任务（这是与远程监控器最大的区别）。在监控程序内处理器完全可以再接收外界的中断和其他触事件，而不是停止运行。这种方式综合了 JTAG 和远程调试的优点，它可以增加以下两个好处：

- 在不禁止中断的前提下调试前景任务（即中断时正在运行的任务）；
- 不用停止处理器的运行就可以读写和修改存储器（对于机电设备非常重要）。

更为强大的是 ARM 的实时跟踪解决方案，它由三部分组成：

- 嵌入跟踪微核；
- 跟踪分析仪；

- 跟踪调试软件。

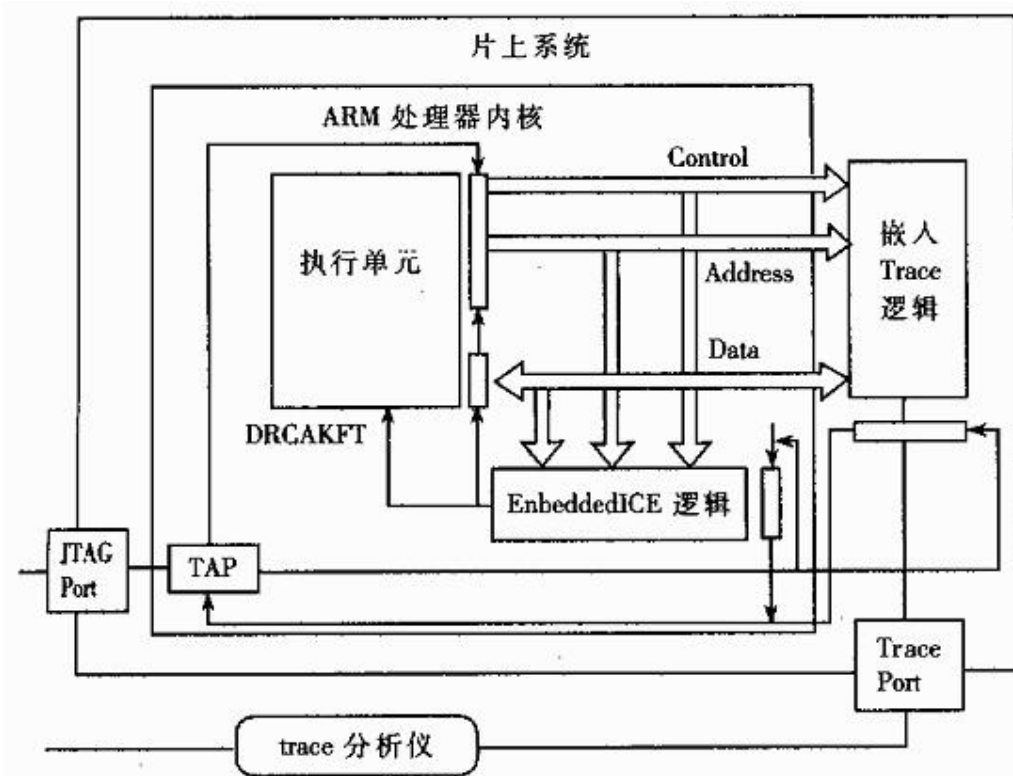


图 4 ARM 的 Trace 调试模式

通过这三种工具可实现完全的实时跟踪。跟踪微核存在于芯片，它可以不停止 CPU 的运行而实时监控芯片总线的信息，并把设定触发范围内的所有信息在 CPU 运行的同时通过压缩的方式送到外部的跟踪分析仪器里。分析跟踪仪器从芯片外部通过跟踪口（另外一个不同于 JTAG 的接口）收取信息。因为是压缩的数据，所以分析仪不需要采用与跟踪微核实时跟踪相同的速度。这大大降低了分析的成本，并增加了存储的容量。而 PC 端的跟踪软件则来自分析仪的数据重新组织起来，从而重现处理器的历史状态和数据、程序流程。同时还可以把执行代码与源代码链接起来，使调试者快速理解跟踪数据。ARM 的这种方式通过芯片内部的实时跟踪硬件加上低成本的分析仪器，解决了传统在线仿真器（ICE）和逻辑分析仪的诸多弊端。其示意如图 4。

### 3 Nexus 标准

自从 JTAG IEEE1149.1 标准出来后，越来越多的高端嵌入芯片生产商开始采用这个标准。但是 1149.1 标准只能提供一种静态的调试方法，如处理器的启动和停止、软件断点、单步执行、修改寄存器，而不能提供处理器实时运行时的信息。于是各个厂家在自己的芯片上，把原有的 JTAG 的基本功能进行了加强和扩展，如前面提到的 E-TRACE、背景调试模式 BDM (Background Debugging Mode) 和片上仿真 OnCE (On-Chip Emulation) 等，在处理器不停止运行的前提下，进行实时的调试。

由于这些增强的 JTAG 版本之间各有差异，而且即使同一厂家的不同产品之间也在存在着不同。所以一些芯片厂商和调试工具开发公司于 1998 年成立了 Nexus 5001 论坛，以期提出一个在 JTAG 之上的嵌入式处理器调度的统一标准。

Nexus 将调试开发分成四级，从第一级开始，每级的复杂度都在增加，并且上级功能覆盖下一级。第一级使用 JTAG 的简单静态调试；第二级支持编程跟踪和实时多任务的跟踪，并欢用户使用 I/O 引脚作为多路复用辅助调试口；第三级包括处理器运行时的数据写入跟踪和存储器的读写跟踪；第四级

增加了存储替换并触发复杂的硬件断点。

从第二级开始，Nexus 规定了可变的辅助口。辅助口使用 3~16 个数据引脚，用来帮助其他仿真器和分析仪之类的辅助调试

工具。其示意如图 5。

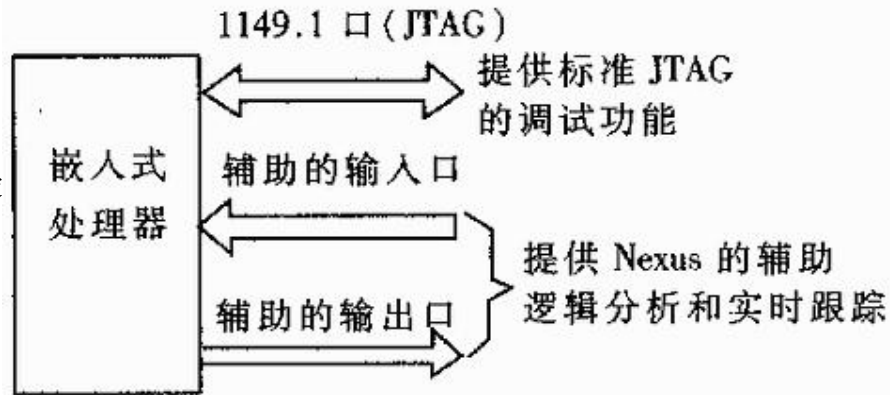


图 5 Nexus 的接口标准

通过 Nexus 标准可以解决以下问题：

- 调试内部总线没有引出的处理器，如含有片内内存器的芯片；
- 传统在线仿真器无法实现的高速调试；
- 深度流水线和有片上 Cache 的芯片，能够探测具体哪条指令被取和最终执行；
- 可以稳定地进行多内核处理器的调试。

#### 4 调试技术的展望

通过上面的分析可以看出，目前的调试技术可以在频率 100MHz、内部总线外部不可见、需要进行实时跟踪的情况下充分发挥优势，弥补传统的远程调试器和在线仿真器的不足，并且成本非常低廉。

同时，调试技术还在不停地发展，目前 IEEE1149.4 标准也已经产生。它主要是将边界扫描结构用于处理模数混合芯片的调试。Nexus 也已经完成了标准的制定并有厂商开始在芯片上提供 Nexus 的调试硬件模块。但是这些标准到底会不会被各个芯片厂商所采用，还有等时机的成熟。特别是两大主流内核公司 ARM 和 MIPS 分别采用自己独特内核调试技术。ARM 采用基于 JTAG 版本的 E-Trace，而 MIPS 则是用 EJTAG——加强的 JTAG 技术。它们对 Nexus 的态度也是旁观等待。

本文内容来自互联网，著作权归原作者所有。由电子零件城 (<http://www.epcity.com/>) 整理并制作成 PDF 文件，仅供个人学习之用，不得用于任何商业目的，否则后果自负。如果您认为本 PDF 文件侵犯了您的任何权利，请来信 [epcity@epcity.com](mailto:epcity@epcity.com) 通知，本站立即删除。

搜集整理：电子零件城-笨笨兔 (QQ: 154502842)      2004-04-10