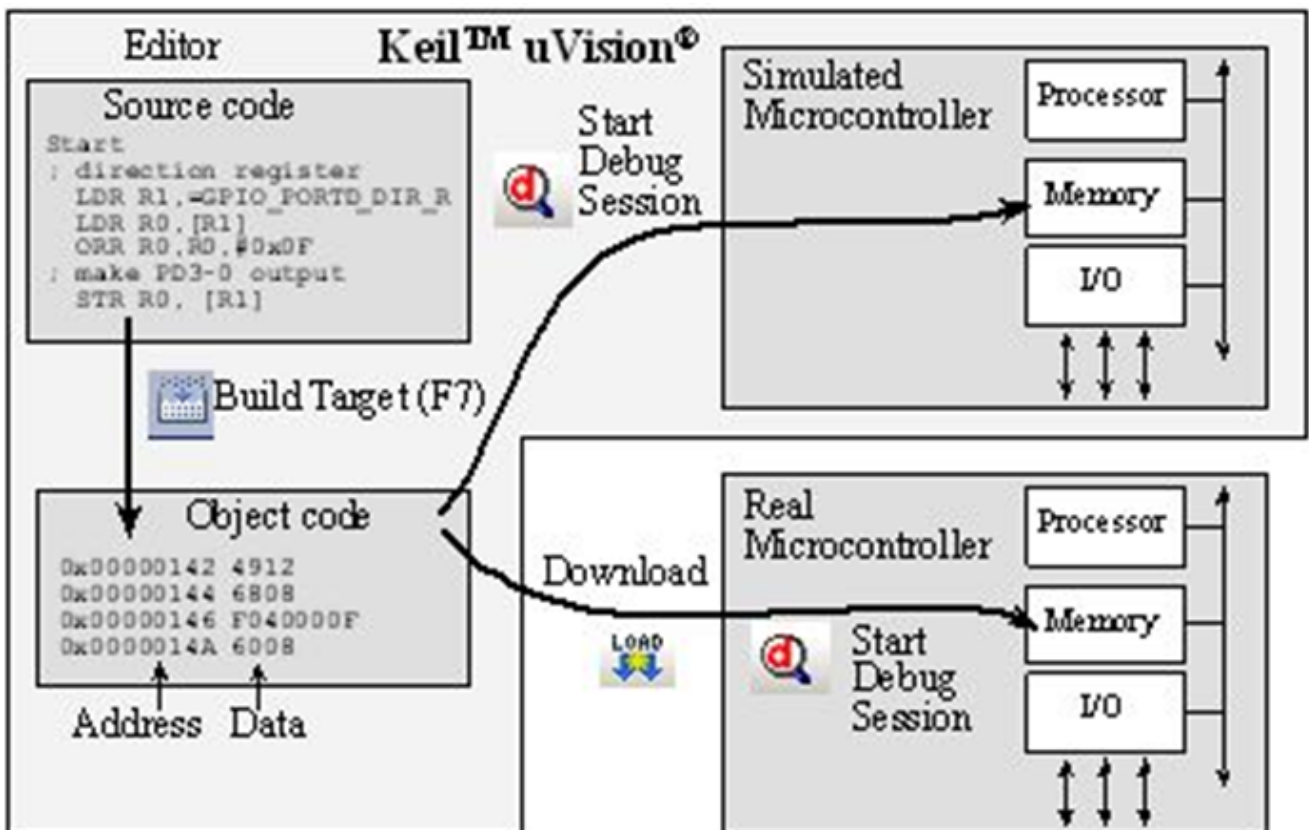


LAB11 FunctionalDebugging

keil简介

Keil 是Keil Software公司出品的51系列兼容C语言软件开发系统，与汇编相比，C语言在功能上、结构性、可读性、可维护性上有明显的优势，因而易学易用。Keil提供了包括C、宏汇编、链接器、库管理和一个功能强大的仿真调试器等在内的完整开发方案，通过一个集成开发环境（ μ Vision）将这些部分组合在一起。Keil软件的运行环境是WIN98、NT、WIN2000、WINXP、WIN10等操作系统。



Keil调试器的使用

1.打开工程

- 解压FunctionalDebugging.zip
- 点击Project->Open Project，选择解压好的路径下FunctionalDebugging文件夹中的.uvproj文件
- 可以看到两个.s文件，Startup.s和main.s

2.开始调试器

- 点击Debug->Start/Stop Debug Session，启动调试器

在调试状态，Debug 菜单项中的命令可以使用了，有关编译的工具栏按钮消失了，出现了一个用于运行和调试的工具栏，Debug 菜单上的大部份命令都有相应的快捷按钮。

从左到右依次是复位、运行、暂停、单步跟踪、单步、执行完当前子程序、运行到当前行、下一状态、打开跟踪、观察跟踪、反汇编窗口、观察窗口、代码作用范围分析、1# 串行窗口、内存窗口、性能分析、工具按钮命令

3.基本调试操作

- 单步跟踪运行
- 全速运行
- 观察 / 修改存储器的数据
- 复位
- 设置断点
- 带断点的全速运行
- 退出仿真

代码运行结果

```
0x20000000: AAB81644 92607E6C 7A08E694 62B04EBC 4A58B6E4 B77DD339 3FC5DB01 C70DE3C9 4F55EB91 D79DF359 00000014 FFA18850 000075EE 00000000
0x20000038: 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
0x20000070: 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
0x200000A8: 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
```

我们先看一下代码的构造部分

```
        THUMB
SIZE      EQU      20
;  RAM Section
        AREA      DATA, ALIGN=2
; Declare arrays to collect instrumentation data
HappyBuf SPACE SIZE      ; 20 instances of happy
SadBuf   SPACE SIZE      ; 20 instances of sad
Cnt       SPACE 4         ; offset(index) into arrays
M         SPACE 4         ; random number store
happy     SPACE 1         ; strategic variables
sad       SPACE 1         ; happy and sad
```

我们可以知道内存的分配：

- 前五段：HappyBuf
- 第六至第十段：SadBuf
- 第十一段：Cnt
- 第十二段：M

我们经过了十四次迭代之后可以发现已经得到了最终结果，所以我们可以得到cnt变量和Happybuf的最终值。所以我们可以得到：

Happybuf:

```
AAB81644 92607E6C 7A08E694 62B04EBC 4A58B6E4
```

Sadbuf:

```
B77DD339 3FC5DB01 C70DE3C9 4F55EB91 D79DF359
```

Cnt:

```
00000014
```

以上就是针对结果进行的分析过程，相对应的可以在memory中找到我们需要的值。

