火控计算机软件执行地址跟踪系统的研究

张　斌，王海晏，于　雷
空军工程大学 工程学院，陕西 西安　710038

摘　要：应用通用技术研制完成了程序存储器板系统执行地址跟踪系统，可以在不对火控系统产生任何影响的前提下，跟踪并记录下火控系统在进入不同工作状态时以及进入后火控计算机软件执行的地址。并且可以根据具体需要完成不同长度的地址跟踪记录。跟踪系统结构设计简单、方法先进，完全满足对该火控计算机的地址跟踪要求，并通过相关单位的质量认证。

关键词：地址跟踪系统；先入先出寄存器；DMA 操作；ISP 器件
中图分类号：V247.1^{+}3　　**文献标识码**：A　　**文章编号**：1009-3516(2000)05-0005-03

现代战斗机火控系统的核心是火控计算机，其软件则是火控计算机的“灵魂”。读出和分析其软件是在火控计算机内加入国产武器的前提和必要条件[1]。在读出程序后，为了减少软件分析的工作量，查清软件的逻辑结构，对软件的流程的分析就显得很有必要，即弄清楚软件的总体思路和执行过程[2]。而软件的执行地址就体现了软件的执行过程。因此，对软件执行地址的跟踪有助于了解软件的执行过程，而软件执行地址跟踪系统的研究正是以针对这一问题为目的的。在国内，相关方面的研究或类似系统的设计中[3]，尚不足以达到实时跟踪记录的要求，又由于各种类型火控计算机的差异，因此，针对机型设计跟踪系统显得十分必要。

1　系统设计原理

火控计算机的软件结构复杂，分枝状态繁多，仅依靠读出的代码通过反汇编来搞清其逻辑结构，困难相当大。但根据火控系统进入不同状态是在人的具体操纵下由计算机控制完成的这一原理，人为地使火控系统进入不同的状态，同时记录下此时火控计算机运行时地址总线上的信息，即火控计算机软件运行过程中动态的地址变化，把这些变化存储成数据文件，以便以后对照从火控计算机中读出的代码，离线分析火控计算机的软件。

2　地址跟踪系统的设计

2.1　硬件设计

跟踪系统的原理框图如图1所示。PC机通过驱动和译码驱动控制逻辑，控制逻辑控制先入先出寄存器的读写，先入先出寄存器的数据端通过插头连接在火控计算机的地址总线上，先入先出寄存器的读写时序见图2、图3。

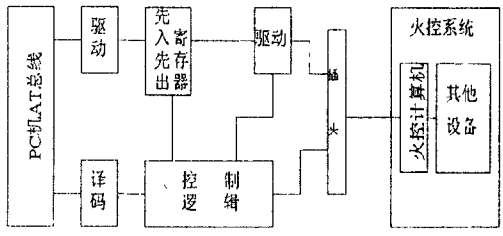

图1　系统原理框图

工作过程是让火控系统进入不同状态，这时火控计算机会进入不同的程序段，这些不同的程序段会以不同的地址反映出来。把这些地址作为先入先出寄存器的数据写入先入先出寄存器，再由PC机从先入先出寄存器中将其读出，有规律地存储在硬盘的各个文件当中，以备分析之用。同时，地址的跟踪长度还可以人为地设置，以方便各种不同场合的需要。

收稿日期：2000-06-18
基金项目：空装外场部科研基金资助项目(KJ98068)
作者简介：张　斌(1962-)，男，四川绵阳人，讲师，主要从事火力控制研究.

图 2 先入先出寄存器读时序

图 3 先入先出寄存器写时序

硬件的设计采用现场可编程门阵列技术、先入先出寄存器和 DMA 技术等手段实现。原理框图见图 1。

先入先出寄存器 CY7C429 见图 4。管脚定义为,/W 是写信号,/R 读信号。与本系统使用有关的还有/HF 为半满标志 /FF 为全满标志 /BF 为空标志[4]。

硬件部分的关键是 DMA 控制与先入先出寄存器 CY7C429 配合使用逻辑部分的电路。该部分电路采用 LATTICE 的在线可编程逻辑器件 ispLSI1016－60,提高了系统的集成度和可靠性。部分内容如下所示[5~6]

```
SIGTYPE DARQ REG OUT;
SIGTYPE DRCLD ASYNC OUT;
SIGTYPE DRRES ASYNC OUT
EQUATIONS
DARQ. PTCLD=DMARQ;
DARQ=D0;
DRCLD=DARQ & ! HF;
DRRES =! DMADND # TC # REST;
END;
```

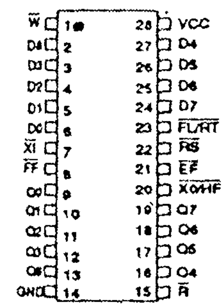

图 4 先入先出寄存器 CY7C429

由于该型火控计算机的地址总线是 16 位地址总线,故 PC 机亦用 16 位 AT 总线操作。把火控计算机的地址总线通过驱动接到先入先出寄存器 CY7C429 上,由 PC 机发出“开始”信号,此时,先入先出寄存器清 0。若火控计算机未工作,则先入先出寄存器 CY7C429 中未被写入数据,也不会有 DMA 请求信号发给 PC 机;若火控计算机工作,则有数据(火控计算机工作的地址信息)写入先入先出寄存器 CY7C429 中。当先入先出寄存器 CY7C429 被写满一半时,它发出半满信号/HF 给 PC 机作为 DMA 请求信号,此时 PC 机响应该 DMA 请求,进入 DMA 模式,将已存入先入先出寄存器 CY7C429 中的火控计算机工作的地址信息读入 PC 机内存中。与此同时,CY7C429 中继续写入火控计算机的地址,这样就不会因为由于写满后再读出而导致后续地址的丢失,又不至于使后写入的信息将以前的覆盖掉,从而保证了地址信息读入的连续性。

2.2 软件设计

软件除对硬件进行一定的设置及驱动外,还可供用户选择进行一定长度的地址记录,并且存成相应长度的二进制文件。每个文件长度可为 128 K 或 64 K,最长可达 20 个文件;还可以进行继续地址的记录,记录长度为 128 K×20 字节。

软件第一部分为 DMA 的设置部分,根据本系统的需要,设置部分如下:

```
    #define Page _ Addr      0x08b //Channel 5's Page _ Address
    #define DMAC             0X0C0 //DMA2's Original I/O Address
    #define Dma _ Request     0x0d0 //The Same Address with Command _ Register
    #define MEM _ ADDR        0x6000
//*********************DMA Setup************************************************
    outportb(0xd4,0x05);  //  Mask Register select ch5 mask bit
    outportb(0xd2,0x01);  //  Clear Request Register
    outportb(0xd8,0x01);  //  Clear First/Last _ Flip _ Flop
    outportb0xc4,low _ byte);//0x00);  //  _ Low 8 _ bits of RAM _ Address
    outportb(0xc4,high _ byte);//0x00);  //  _ High 8 _ bits of RAM _ Address·0000H
```

第二部分为根据用户需要,产生必要的控制信号,读数据并存储成一定的文件形式。另外,DMA 的重设也是软件中值得注意的问题。

2.3　跟踪系统对火控系统的影响

如图 1 所示,地址跟踪系统仅仅通过一根电缆通过插头联入火控系统的地址总线上,相当于在火控系统的地址总线上接了一个上"三通",原地址总线不变,因此其系统工作不会受到任何影响。

2.4　跟踪系统记录的某次运行地址段

运用本地址跟踪系统所跟踪捕获到的某火控计算机运行当中的一段程序的地址情况如下。

5C99 5D99 5E99 5F99 0099 0199 0299 0399 0499 0599 0699 0799 0899 0999 0A99 0B99 0C99
0D99 0E99 0F99 1099 1199 1299 1399 1499 1599 1699 1799 1899 1999 1A99 1B99 1C99 1D99
1E99 1F99 4099 4199 4299 4399 4499 4599 4699 4799 4899 4999 4A99 4B99 4C99 4D99 4E99

以上为本系统读出的地址内容片段。从这段数据可以看出:高 8 位地址为 99H,低 8 位地址从 5CH 执行到 5FH,之后跳转到 00H 后又执行到 1FH,之后跳转到 40H,等等。因此,从这些记录的数据可以分析出此段程序的运行情况,说明本系统能够达到对软件地址进行跟踪的目的。

3　结束语

本系统经实际使用,能够达到预期的目的。使用过程、实用性和据此得出的某型火控计算机的运行地址,均已通过相关单位的质量认证,效果良好。经过国内相关单位和资料的查新,本系统设计方法有独到之处,且可靠性高,并不影响原系统工作。此外,本系统设计的思想对于类似的地址跟踪装置或高速数据采集系统同样有借鉴之处。

参考文献:

[1] 李春亮. 火控计算机软件可靠性实验初探[J]. 洛阳:火力与指挥控制,1990,15(3):7-10.
[2] 李春亮. 火控计算机的软件支持[J]. 洛阳:火力与指挥控制,1992,17(1):25-30.
[3] 樊水康. 标准工业总线的 32 位失控计算机系统研究[J]. 火力与指挥控制,1998,23(2):34-39.
[4] 李继灿,李华贵. 新编 16—32 位微型计算机原理及应用[M]. 北京:清华大学出版社,1997.
[5] 齐怀印,卢锦. 高级逻辑器件与设计[M]. 北京:电子工业出版社. 1996.
[6] Douglas L Perry. VHDL 电子设计硬件描述语言[M]. 北京:学苑出版社. 1994.

Analysis of Address Tracing System of Fire Control Computer

ZHANG Bin,　WANG Hai-Yan,　YU Lei
(Engineering Institute, AFEU., Xi'an 710038, China)

Abstract: It will be helpful for analyzing, understanding and grasping the soft structure and its course of Fire control computer by tracing the execute address of the computer software, thus meaningful to patching up the original software. The execute address tracing system using ISP and DMA can trace and record the extcute address of the Fire control computer at different status. Forthermore, the tracing system can take the different length address tracing recording according to the specific requirement.

Key words: address tracing system; FIFO register; DMA operation; ISP device