文章编号：1007-1180(2010)09-0052-07

1553B 总线通讯的可靠性设计

代 霜，王 槐，徐抒岩
（中国科学院 长春光学精密机械与物理研究所，吉林 长春 130033）

摘 要：为保证通讯的正常时序和避免空间环境 [尤其是单粒子翻转效应（SEU)] 对 1553B 总线通讯的危害性影响，建立了 1553B 总线通讯通用的失效模式分析模型。针对不满足通讯时序而引起的通讯失效，通过增加握手时序的方式加以避免。软件设计中针对典型的失效模式，如中断无法响应、帧格式错误等，给出与一般通讯软件不同的高可靠性软件设计流程，具体在设计方法上采取寄存器定时更新、存储区表决法以及冗余设计等可靠性措施避免失效，并通过对固定位置的存储单元模拟 SEU 故障注入的方式进行验证，降低了单粒子翻转的危害性，提高了 1553B 总线通讯的可靠性，具有普遍意义。

关键词：1553B 总线通讯；单粒子翻转；失效；可靠性
中图分类号：TP336 **文献标识码**：A
DOI：10.3788/OMEI 20102709.0052

Communication Software Reliability Design of 1553B Bus

DAI Shuang, WANG Huai, XU Shu-yan
(*Changchun Institute of Optics, Fine Mechanics and Physics, Chinese Academy of Sciences, Changchun* 130033, *China*)

Abstract: For the sake of accurate communication scheduling and avoiding harmful effect of SEU, the failure model of 1553B bus communication is given. In order to meet the requirement of communication scheduling, the way of handshake is proposed. Then the reliable software dataflow is given for SEU (Single event upset), unlike common communication software, some measures are taken such as register renewed periodically, memory voting and redundancy design. Finally, the fault injection is applied to validate. Practical results show that the design is necessary and effective.

Keywords: 1553B bus; single event upset; fault tree; reliability

1 引 言

目前,1553B 总线通讯被星上系统普遍采用[1]。1553B 总线通讯负责接收星上系统的外部控制数据,并下行表征系统内部重要运行状态的数据,是星上系统与外界沟通的桥梁,为保证星上系统顺利完成任务,必须保证 1553B 总线通讯的准确可靠。而 1553B 总线通讯软件最重要的特点是受空间环境辐射效应的影响[2]。就目前的认识而言,影响较大的辐射效应主要有:总剂量效应、单粒子效应、航天器表面充放电效应、高能电子内带电效应、太阳电池等离子体带电效应等,其中对 1553B 总线通讯软件造成直接影响的是单粒子效应中的单粒子翻转(SEU – Single event upset)事件。单粒子翻转可引起器件电性能状态的改变,造成逻辑器件或电路的逻辑错误[2],例如,存储器中数据发生翻转,进而引起逻辑功能混乱,计算机程序“跑飞”,甚至造成灾难性的后果;对于通讯软件,可使通讯接口芯片的存储器或寄存器的 0、1 状态发生翻转,从而使系统通讯逻辑混乱,进而使整个系统无法与外界通讯,无法正常执行任务。

本文主要从保证通讯时序的可靠性和对空间环境辐射效应中的单粒子翻转采取相应的可靠性措施两方面,保证 1553B 总线通讯的可靠性。

2 系统组成

本系统中 CPU 采用 ADSP21060,1553B 接口芯片采用 BU65170,具体系统硬件连接如图 1 所示。以 ADSP21060 为 CPU 的主控制器在整个系统中的 1553B 通讯中作为 RT 端,通过 1553B 协议芯片 BU–65170 与 ADSP21060 连接。BU–65170 主要的控制信号有 SELECT, MEM/REG, RD/WR, STRBD, INT 等。其中通过 ADSP 存储区选择控制信号 MS2# 作为 BU–65170 的片选 SELECT; ADSP21060 地址线 A22 作为 65170 芯片的寄存器和存储器的选择信号 MEM/REG;1553B 信号通过两个变压器最后送至传输线上。

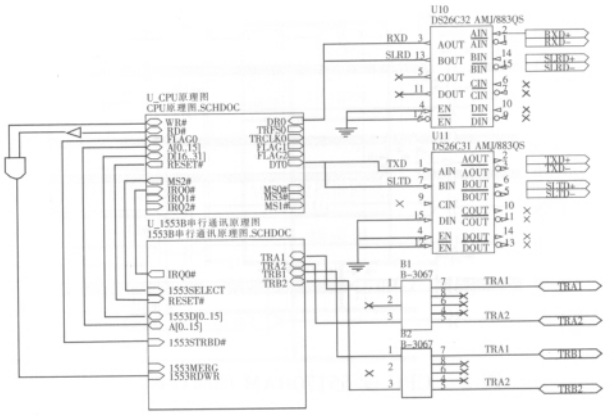

图 1 ADSP21060 与 1553B 总线连接图

2.1 典型总线通讯时序失效分析

上述系统在进行 1553B 总线通讯接口测试时,当上位机向本系统发送包头为“7788H”和“4412H”、其余为“ABABH”的 64 字节数据注入后,经本系统下行后,工作时刻的时间码高字出现异常的“FFFFH”,正常应为“ABABH”。

通过对通讯时序的分析,定位为硬件设计缺陷,没有将 CPU 的 READY 信号与 BU65170 的 READY 信号相连,从而导致 CPU 与 BU65170 之间无握手信号,导致读取异常数据。

由于 BU65170 的 RAM 为双口 RAM,BU65170 的内部存储器管理逻辑和 CPU 都会访问 BU65170 的 RAM。由 BU65170 手册可知,当二者有竞争访问时,SELECT 和 STRBD 同时持续时间 $t2$ 最大为 2.8 μs,没有竞争访问时,$t2$ 最大为 107.5 ns;$t1$ 的最小值为 170 ns,$t1$ 的最大值为 205 ns;在没有竞争访问时 $t1+t2$ 最大为 312.5 ns,在有竞争访问时,$t1+t2$ 最大为 3.005 μs,具体如图 2 所示。

而采用的 CPU 为 ADSP21060,与 1553B 控制芯片 BU65170 之间没有握手信号,CPU 对 BU65170 的访问时间完全取决于内部等待时间,而 ADSP21060 的最大等待周期为 6,其时钟周期为 50 ns,因此,CPU 对外围设备的访问时间为 50×(6+1)=350 ns,从上述分析可以看出,大于前述的 312.5 ns 而小于 3.005 μs,

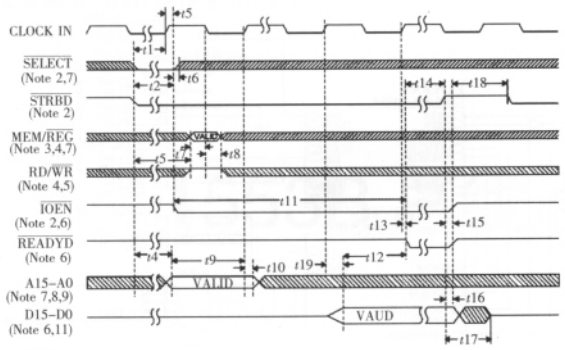

图 2 CPU 读 65170RAM 的时序图

因此，在没有竞争访问时，该访问时间可以保证 CPU 读取到有效数据；然而，如果发生竞争访问，则 CPU 就有可能读取不到有效数据。

针对上述因为握手时序而导致通讯内容异常的问题，修改硬件设计，将 BU65170 的 READY 信号处理后与 CPU 的 READY 信号连接，形成握手信号，保证读操作的时序。经过测试，没有出现上述现象。

2.2 1553B 通讯软件失效模式分析

与一般总线通讯相同，1553B 通讯软件功能主要有通讯初始化功能、接收功能、发送功能及中断处理等功能。然而，由于 1553B 通讯软件时序问题或受空间环境的影响，会引起数据流或控制流的错误[3]，当发生时序错误或单粒子翻转而使存储器数据发生 0 或 1 的跳变时，导致帧格式错误或关键变量错误，从而使读写过程中传递错误信息，进而使接收或发送的数据失效。另一方面，发生单粒子翻转而使寄存器和存储区初始化遭到修改，则会使中断无法响应，也会产生读写数据失效。针对上述情况，本文进行了与一般通讯软件不同的失效模式分析，建立了如图 3 所示的 1553B 通讯软件故障树。从图中可以看出，导致通讯软件失效的中间事件为接收或发送数据失败和读写过程中传递错误信息。子事件有初始化寄存器错误、中断无法响应、帧格式错误、关键变量错误等。

上述典型的失效模式在下面设计通讯软件的过程中会具体加以相应的可靠性设计措施。

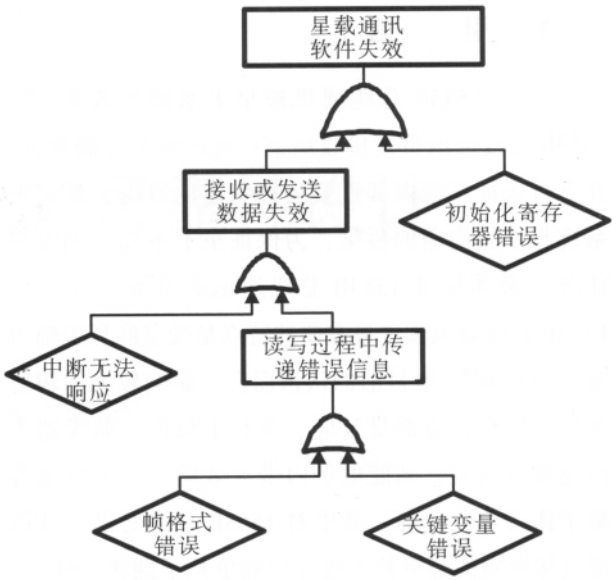

图 3 1553B 通讯软件故障树

3 1553B 通讯软件的组成

3.1 1553B 通讯软件拓扑结构

参考 ISO 网络七层模型，与一般通讯软件相似，将 1553B 通讯软件的总线通讯分为 4 层：物理层、数据链路层、驱动层和应用层[4]，如图 4 所示。物理层按照特定总线协议规定的编码格式进行传输。数据链路层按照特定总线协议规定的数据格式进行传输。总线 MBI 包括 MBI 底层驱动程序和 MBI 通讯程序。一般总线通讯有专用的协议芯片支持。MBI 底层驱动程序实现 MBI 初始化，协议芯片的中断，RAM 地址、寄存器地址设置，内部自测试等功能。MBI 通讯程序根据 MBI 底层驱动程序以及载荷通讯需求接口数据单（ICD）生成，完成协议芯片的初始化、管理以及总线数据接收发送功能。不同于一般通讯软件的是，对其中 MBI 底层驱动程序和 MBI 通讯程序要进行相应的可靠性设计。

3.2 1553B 通讯软件设计流程

对于软件来说，软件工程化技术是保证软件可靠性的基础，它提出了软件开发的基本原则和要求。例如，由不同人员完成软件设计、程序编码和软件测试，保留设计文档、框图和测试记录，使软件的

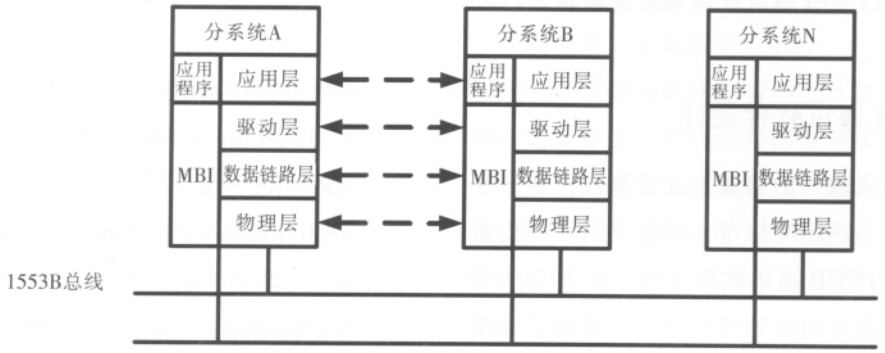

图 4 通讯软件拓扑结构

开发和使用具有可追溯性。由于软件规模和复杂度是影响软件可靠性的一个主要因素，在软件设计中采用自顶而下和模块化的设计方法，可以合理划分模块，实现低耦合高内聚的要求，降低系统实现难度，有利于提高软件的可靠性[2]。

对于 1553B 通讯软件，除了依循上述的一般设计原则外，根据其特点，给出如图 5 的设计流程。主要包括 ICD 表的设计、MBI 底层驱动的开发和 MBI 通讯程序设计。首先应确定总线传输的数据量及周期，主要通过载荷通讯需求接口数据单（ICD）完成此项功能。其中 ICD 的内容主要包括上行的定义、下行参数的定义（包括单位，取值范围等）、参数地址分配以及周期的确定等。对于一些关键参数还要进行针对空间环境的可靠性设计。MBI 通讯程序在 MBI 驱动程序的基础上利用 ICD 对通讯所需的时间和空间资源进行分配，将周期性的通讯任务和非周期性的通讯任务划分开，采取合理的调度方法，保证通讯满足系统设计的要求，进而完成通讯程序

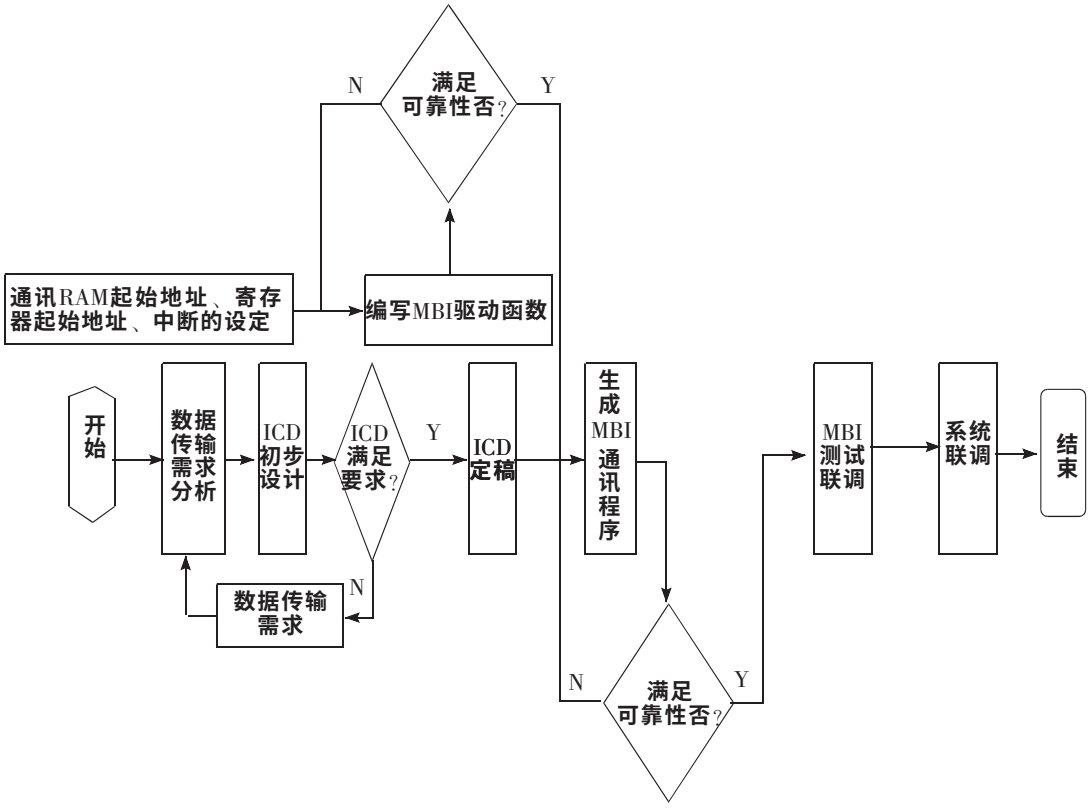

图5 1553B通讯软件设计流程图

的设计。最后通过 MBI 测试联调和系统联调进行验证和完善。

4 1553B 通讯软件设计

按照上述通讯软件的组成及开发流程，根据空间辐射中的单粒子翻转的特点，以在空间环境普遍应用的 RT 端的 1553B 通讯软件为例，在 ICD 的编写、MBI 底层驱动和 MBI 通讯程序中主要对关键参数、数据存储、寄存器设置等几个方面进行可靠性设计。

4.1 1553B 通讯软件 MBI 实现

以 RT 端的软件为例，针对 BU-65170 芯片，主要实现了以下几个方面的功能：

(1) 配置寄存器的初始化

实现了主要工作模式的设定、存储方式的选择及中断方式设定等。

(2) 消息存储方式的选择和存储地址的分配

存储方式主要有单缓冲、双缓冲、循环缓冲方式。对于发送的消息根据消息块的大小可以选择不同的存储方式。数据块小于 32 字的选择单缓冲方式，数据块大于 32 字应选择循环缓冲方式。对于接收的消息，一般选用双缓冲方式；但是，对于发送周期间隔小或消息长度长（大于 32 字）的应选用循环缓冲方式。

(3) 对于非法消息设置非法化表

设置非法化表是保证 1553B 通讯可靠性的方法，可以将不满足预先设定的子地址和消息块长度的消息设定为非法消息，在通讯中这类消息将被芯片自动排除。

(4) 消息中断的处理

消息中断主要实现了数据的移动。对于接收消息，将在接口芯片上的消息移至用户处理区内。对于发送消息，则要求预先将消息移至设定的接口芯片缓冲区，然后置相应的服务请求位。

下面是以子地址 3 接收 32 个字、广播方式，子地址 5 接收 5 个字、广播方式，子地址 1 发送 21 个字为例的 1553B 通讯软件初始化 Rtinit () 的示例代码：

```
/* 寄存器初始化 */
AceRegWrite (CONFIG_3_REG,0x8000);
//设置 RT 为禁止运行模式
AceRegWrite (INTERRUPT_MASK_REG,0x0010);
// 允许消息结束中断
AceMemWrite ((int *) StackPtrA,0);  // 置堆栈指针为 0
AceRegWrite(CONFIG_1_REG,0x0cf80);
AceRegWrite(CONFIG_3_REG,0x8019);
AceRegWrite(CONFIG_2_REG,0x981a);
AceRegWrite(CONFIG_4_REG,0x0000);
AceRegWrite(CONFIG_5_REG,0x0700);
/* 接收和发送缓冲区的地址初始化 */
AceMemWrite
((int *) 0x0143, (int) AddrR3) ;
// 设定 R3 存储区首址
AceMemWrite
((int *) 0x0145, (int) AddrR4) ;
// 设定 R5 存储区首址
AceMemWrite
((int *) 0x0161, (int) AddrT1) ;
//设定 T1 存储区首址
/* 存储方式的设定 */
AceMemWrite
((int *) 0x01a1,0x4000) ;
//T1 单缓冲方式 ;
AceMemWrite
((int *) 0x01a3,0x8200) ;
// R3 双缓冲方式
AceMemWrite
((int *) 0x01a4,0x8200) ;
// R5 双缓冲方式
/* 非法化表的设定 */
AceMemWrite
```

```
((int *) 0x03c3,0x0ffdf) ; //T1 21word
AceMemWrite
((int *) 0x0306,0x0fffe) ;
//R3 32word 广播方式
AceMemWrite
((int *) 0x0308,0x0ffdf) ;
//R4 5word 广播方式
```

其余设定为 0xffff;

初始化芯片后，编写适当的通讯中断程序即可正常进行通讯，这里不再详述。

4.2 1553B 通讯软件可靠性设计

4.2.1 ICD 表的设计

关键变量的定义不能采用一位来表示，尤其不能用 0、1 来表示不同的状态，一般应采取多位来表示。如设置系统加电标志=0x5a5a，表征未加电，0x6161 表示已加电。

4.2.2 MBI 可靠性设计

对于 MBI，一方面需要对取值的合法性进行判断；另一方面，下文将采取存储区表决法来消除单粒子翻转造成的影响。而中断无法响应或初始化寄存器错误将采取定期更新的方式。

(1) 将接口芯片初始化相关的寄存器和存储区定期更新

对一些关键寄存器，如接口芯片的控制寄存器，如果发生单粒子翻转，将使整个通讯接口芯片失灵。而中断屏蔽寄存器的相应位发生翻转，可能会使中断服务请求得不到响应。对这些寄存器应采取定期更新的方法，以避免寄存器值发生跳变造成的后果。

由于通讯芯片的寄存器在更新期间将无法进行正常通讯，因此应考虑在整个大系统内通过广播消息，如系统维护命令，统一进行定期更新，并在更新期间内停止通讯。

(2) 数据存储区的表决选取

将接收的数据存放在 3 个存储区上，然后采用三取二的原则来选择数据。

(3) 数据冗余设计

关键变量主要包括大循环控制变量、有限状态机控制变量、重要的全局指针、重要的全局标志等。上述变量关系到程序运行的总体进程，发生单粒子翻转的概率比一些临时局部变量大很多，造成的后果更严重。采用数据冗余设计的方法可降低发生翻转的概率。以全局变量 iSystemState 的设计为例具体说明如下：

未采用冗余时：

```
if (iSystemState==0x33)
  {
      // 执行信号处理
      iSystemState=0x55;
}
```

采用冗余后：

```
iSystemState = voter (is1,is2,is3) ;
if (iSystemState==0x33)
{

  //执行信号处理
  iSystemState=0x55;
  is1= iSystemState;
  is2= iSystemState;
  is3= iSystemState;
}
```

采用冗余方法，通过复制变量 iSystemState，在使用时用 is1，is2，is3 的多数表决（3 取 2），增加了关键变量 iSystemState 的可信度。

4.2.3 其它

从整个 1553B 总线通讯软件可靠性考虑，还应对程序存储区进行验证，比较常用的方法是对整个程序代码进行求和校验[5]，并将结果作为常量存储在 3 个位置，程序引导到 RAM 时，对程序区进行校验，并将结果与 3 个校验值的表决结果比较，如果两者不一致，应考虑重新引导。考虑到程序可能受到干扰，还应加软件陷阱和软件看门狗。

5 验 证

通常采用故障注入的方法[6]对采取的可靠性措施进行验证。对固定位置的存储单元模拟 SEU 故障注入，应用程序对此单元进行读操作时，监视应用程序的运行状态，从而可以判断应用程序对此位置的故障处理能力[3]。

6 总 结

本文从可靠性角度出发，根据通讯时序和空间环境的特点，针对 1553B 总线通讯提出了一般的设计流程，并提出了有效的防单粒子翻转的设计，此种方法提高了 1553B 总线通讯的可靠性。

参考文献

[1] 赵昶宇, 于平. 基于 LabVIEW 的 1553B 通讯的设计与实现[J]. 光机电信息, 2009, 26(5): 23–26.
[2] 段星辉, 华建文, 代作晓, 等. 一种提高星载软件可靠性的开发方法[J]. 计算机工程, 2009, 35(12): 73–75.
[3] 刘海峰. 星载软件容错设计及验证技术[J] . 中国电子科学研究院学报, 2009, 4(3): 313–316.
[4] 代霜, 王槐, 徐抒岩, 等. 一种多总线通讯系统的实现[J]. 计算机测量与控制, 2009, 17(9): 1834–1836.
[5] 袁春如, 廖泰安, 贺红卫. 基于测试覆盖的嵌入式软件可靠性评估 [J]. 计算机工程与设计, 2009, 30(9): 2198–2200.
[6] 龚健, 杨孟飞. 一种星载控制计算机智能容错方法[J]. 空间控制技术与应用, 2008, 34(6): 29–33.

作者简介： 代霜(1982–)，女，汉族，吉林东丰县人，硕士，助理研究员，2006年于中科院长春光机所获得硕士学位，主要从事嵌入式系统设计研究。 E–mail: dai–dai123@163.com

钟敏霖当选美国激光学会会士

美国激光学会（LIA）执行委员会投票选举清华大学钟敏霖教授为学会会士（LIA Fellow），以表彰他为国际激光加工学术界和美国激光学会作出的贡献。授称号仪式将于9月在美国加州举办的国际激光与光电子学应用会议（ICALEO 2010）上进行。

美国激光学会成立于1968年，是国际激光、激光加工和激光安全领域的权威机构，每年举办ICALEO等大型国际会议，会员遍布全球各地。

自1968年成立以来，美国激光学会共授予约80人Fellow称号，其中包括几位诺贝尔奖获得者。据了解，钟敏霖教授是美国激光学会授予Fellow称号的第一位来自中国大陆的学者。