文章编号：1005-8451（2015）04-0048-06

高效的双CPU系统安全数据交互机制的应用

徐　军，孙军峰，张　磊
（卡斯柯信号有限公司　研发中心，上海　200071）

摘　要：轨道交通行业中的嵌入式设备对系统安全性要求高，系统交互数据的安全性尤其重要。根据安全相关系统的安全性特点和需求，提出了一种基于双口RAM的双CPU系统安全数据交互机制，经过在实际项目中应用，可以满足轨旁安全系统中数据传输的安全、可靠、实时、高速传输数据的需求。

关键词：安全数据；双口RAM；自检；角色轮换
中图分类号：U285：TP39　**文献标识码：**A

Application of safety data-exchange mechanism of Double-CPU System

XU Jun, SUN Junfeng, ZHANG Lei
(Research and Development Center, CASCO Signal LTD., Shanghai　200071, China)

Abstract: Embedded devices required high security system. The safety of data exchange in railway industry was extremely important. According to the characteristics and needs of the security, the paper proposed safety data-exchange mechanism of double-CPU System based on dual port RAM. The mechanism was applied in actual project, and could meet the needs of safe, reliable, real-time and high-speed data transmission in trackside safety system.

Key words: safety data; dual-port RAM; high speed; role cycling

轨道交通行业中，一些安全相关系统具有多块板卡，各个板卡负责不同的功能，并组成多CPU系统。各个CPU之间存在复杂的数据传输过程，为了提高系统的整体安全性，需要保证各个CPU系统之间传输的数据安全可靠，并且能够高速实时地交互，如果数据传输通道出现故障或者失效，导致交互的数据不能满足安全性要求，最终影响整个设备或者系统的安全性，甚至引起灾难性后果[1]。

这些安全相关系统依赖于安全数据来控制整个系统的运行，并应用双口随机存取存储器（Random Access Memory，RAM）作为安全数据高速传输通道[2]，交互大量的安全相关数据，包括状态信息和控制命令等。根据双口RAM的工作原理，双口RAM两端的控制芯片需要相互配合，共同完成数据的交互，硬件电路设计复杂，同时对数据访问、地址译码、芯片控制的要求高，基于双口RAM的数据交互过程成为了系统安全性的薄弱环节，双口RAM在数据交互的过程中可能存在各种故障或者失效，包括系统性失效和硬件随机失效[3]。

收稿日期：2014-09-10
作者简介：徐　军，助理工程师；孙军峰，高级工程师。

在安全相关系统中使用双口RAM进行数据通信时，必须满足以下3个条件：

（1）避免双口RAM的两端板卡发生访问冲突；

（2）提高双口RAM的数据交互速度，不影响设备的数据通信量；

（3）保证在双口RAM中存储的数据完整性、正确性、可靠性。

依据上面的分析，本文将双口RAM的数据交互过程进行安全性设计，对双口RAM的系统失效和硬件随机失效进行防护，降低系统的失效率，提高系统的安全性。

本文结合具体的轨旁安全平台系统安全性要求和双口RAM机制，设计了一种双CPU系统安全数据交互机制，可以满足轨旁安全平台系统数据传输的安全性和实时性要求。

1　系统架构

本文中提到的轨旁安全平台系统主要用于轨道安全系统中轨道设备状态采集与地铁状态控制。该设备实时的采集轨道设备状态与地铁列车车载控制器的运行状态，同时该设备将控制命令发送给轨道

设备与地铁列车车载控制器，来控制整个地铁的正常运行，该系统设备对数据传输的安全性、可靠性、实时性要求高。该系统由主处理板 MPU、高速通信板 HCU 组成。

MPU 与 HCU 通过双口 RAM 交换系统的各种安全通信数据。数据交换框图如图 1 所示。

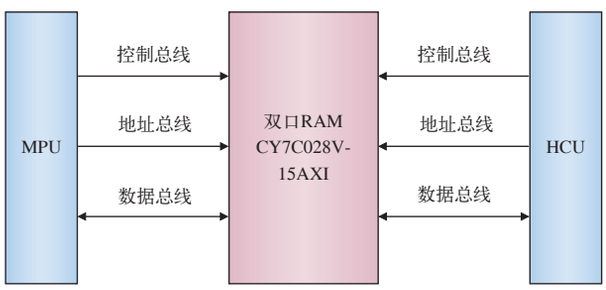

图1　数据交换框图

轨旁安全平台系统中采用的双口 RAM 芯片为 CY7C028V-15AXI，最高读写速度为 15 ns，数据容量为 64 K x 16 bit。

双口 RAM 连接 HCU 板的一端为 MPC8247 的 LOCAL BUS 总线，连接 MPU 板的一端为 CPCI 总线桥接芯片的 LOCAL BUS 总线，HCU 可以直接通过 LOCAL BUS 总线访问双口 RAM，而 MPU 板通过 PCI 总线访问。其中还有控制信号，如片选、读写、中断、BUSY 信号等，双口 RAM 交互电路图如图 2 所示。

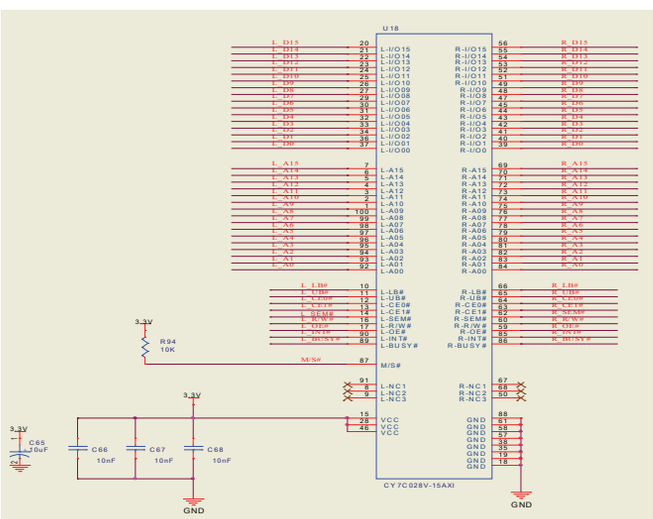

图2　双口RAM交互电路图

MPU 作为逻辑运算和控制模块，负责对接收的安全数据进行逻辑处理，并产生相应的结果，控制整个系统安全的运行。HCU 作为数据通信接口，从外部接收或者采集系统的运行状态数据，并传递给 MPU，同时将 MPU 产生的结果数据发送给相应的执行机构或者外部设备。

双口 RAM 是 MPU 板和 HCU 板之间的数据交换空间，可以完成大批量、实时的数据交换。MPU 板与 HCU 板之间交互的数据是安全相关数据，必须保证在双口 RAM 中存取数据的完整性、正确性、可靠性，显得尤其重要。

应用于轨旁安全平台系统中的双口 RAM，不仅要的避免多 CPU 访问共享双口 RAM 而引起的冲突问题，解决数据通信瓶颈问题，同时应该能够预防由双口 RAM 功能故障或者硬件失效而引起的数据失效或丢失，满足轨旁安全平台系统的安全性和可靠性要求。

针对以上要求，本文提出了一种基于角色变换和自检技术的双口 RAM 数据安全、高效通信方案。

2　安全数据交互机制

为避免 MPU 和 HCU 同时对双口 RAM 的同一个内存单元进行访问，本设计没有采用双口 RAM 的中断或者信号量等机制，而是采用了一种基于角色的环形缓冲收发机制，将双口 RAM 的划分为两个独立环形缓冲区：发送环形缓冲区和接收环形缓冲区。

发送环形缓冲区负责将 MPU 传递给 HCU，最终发送给外部设备；HCU 从外部设备接收到数据，放到接收环形缓冲区，并传递给 MPU。

本设计将整个 128 kbit 的双口 RAM，分为数据交互区和状态交互区，双口 RAM 进行角色功能分区示意图如图 3 所示。

其中，数据交互区用于 MPU 与 HCU 交换通信数据，其大小为 126 kbit，将数据交换区分为上下环形缓冲区模块，大小都为 63 kbit，上模块为发送环形缓冲区，下模块为接收环形缓冲区。

发送环形缓冲区分为 A、B、C 共 3 个区块，每个区块的大小都为 21 kbit，每个区块轮流性地被设置为 3 种角色：写入区块、读出区块、测试区块。

接收环形缓冲区分为 D、E、F 共 3 个区块，每个区块的大小都为 21 kbit，每个区块都轮流性地设

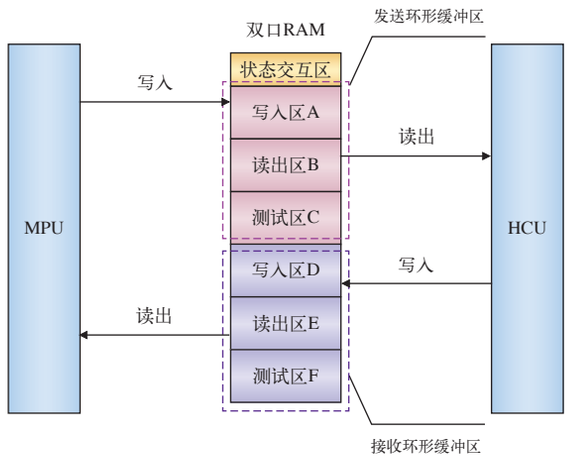

图3　双口RAM功能角色示意图

置 3 种角色：写入区块、读出区块、测试区块。

状态交互区的大小为 2 kbit，用作 2 个 CPU 系统交互状态信息和告警信息。

2.1　系统数据处理

轨旁安全平台系统的主逻辑运算模块的运行周期为 600 ms，该模块按照周期进行数据接收、数据处理、数据输出。

在第 个周期，MPU 上的控制逻辑运算模块从双口 RAM 接收到数据后，放到逻辑接收缓冲区；从逻辑接收缓冲区取出 个周期的数据并进行逻辑处理；将 个周期的逻辑处理结果，从逻辑发送缓冲区中取出，并放到双口 RAM 中。

MPU 上的控制逻辑运算模块对安全数据进行逻辑处理的时间不超过 300 ms，如果逻辑处理时间超过 300 ms，就会影响 MPU 接收或者发送数据。

同样，MPU 上的控制逻辑运算模块接收、发送数据超过 300 ms，也会影响逻辑处理功能。在接收发送处理阶段，300 ms 中的 280 ms 时间，被分为 20 个发送接收子周期，每一个子周期的时间为 14 ms。

在 HCU 中，也是按照同样的运行节拍，从双口 RAM 中写入或读出数据。

MPU 与 HCU 之间交互的数据，按照预先定义的双口 RAM 交换数据帧进行。

2.2　双口RAM功能处理

双口 RAM 的发送与接收环形缓冲区的 3 个区块，在任意一个周期，只能处于读出、写入、测试 3 种角色之一，而且区块角色进行周期轮换，如表 1 所示。

表1　区块角色轮换表

发送环形缓冲区			接收环形缓冲区			周期
区块A	区块B	区块C	区块E	区块D	区块F	
W(M)	R(H)	T(H)	W(H)	R(M)	T(M)	1
R(H)	T(H)	W(M)	R(M)	T(M)	W(H)	2
T(H)	W(M)	R(H)	T(M)	W(H)	R(M)	3
W(M)	R(H)	T(H)	W(H)	R(M)	T(M)	4
……	……	……	……	……	……	……

（1）W(M)：角色为写入区块，且 MPU 向区块写入数据；（2）R(H)：角色为读出区块，且 HCU 从区块读出数据；（3）T(H)：角色为测试区块，且 HCU 对区块进行测试；（4）W(H)：角色为写入区块，且 HCU 向区块写入数据；（5）R(M)：角色为读出区块，且 MPU 从区块读出数据；（6）T(M)：角色为测试区块，且 MPU 对区块进行测试。

MPU 与 HCU 通过双口 RAM 区块角色进行数据交互的步骤如下：

（1）在 2 个 CPU 系统启动后，进行初始化。同时时钟模块初始化后，为 2 个 CPU 提供统一的时钟信号，时钟模块会提供 1ms 周期的时钟信号，在 2 个 CPU 模块上产生外部时钟信号中断，2 个 CPU 模块对中断进行计数。（2）读出区块内容是否读完，如果读完，将该区块设置的标志变换为测试区块，下个周期对该区块进行测试。（3）写入区块内容是否写完，如果写完，将该区块设置的标志变换为读出区块，下个周期对该区块进行读出。（4）测试区块内容是否测试完，如果测试完，将该区块设置的标志变换为写入区块，下个周期可以对该区块进行写入。（5）对测试区块进行检测，是否发现硬件随机失效，若有在状态交互区中进行记录状态和告警信息。（6）当时钟信号计数值达到 600 ms，就为一个接收发送周期，对 3 个区块的角色进行轮换。

MPU 与 HCU 通过相同的外部时钟中断来驱动数据处理软件模块的运行，MPU 与 HCU 在对双口 RAM 进行访问时可以做到同步、流水线作业。

在同一个处理周期内，发送环形缓冲区或者接收环形缓冲区中任何一个区块，都有明确固定的角色，MPU 板和 HCU 板不会同时访问操作相同区块，只有一个板卡对特定区块进行访问。避免了双口 RAM 的访问冲突问题，不需要另外的采取硬件仲裁、

软件仲裁或者信号量交互等手段。

为了保证双口 RAM 本身功能的可靠性以及存储在其中数据的安全性，通过分周期和角色对相应区块的存储单元进行功能性检测，提高了双口 RAM 的可靠性，具体双口 RAM 存储单元检测见下节。

2.3 双口RAM检测

系统运行的过程中，采用相应的算法对双口 RAM 电路系统性故障和硬件随机失效进行检测，可以对双口 RAM 电路用到的数据线、地址线、控制进行检测，可以有效的发现失效故障的电路和内存单元。对双口 RAM 检测分为 2 个步骤：上电自检和在线检测。

嵌入式设备的板卡上电后，bootloader 开始对系统板卡硬件进行初始化，在 bootloader 初始化完 CPU、内存、时钟等硬件后，bootloader 使用 Abraham 算法对双口 RAM 进行全面的检测。

在 bootloader 测试双口 RAM 通过后，开始引导操作系统运行，在系统正常运行过程中，按照系统角色周期性的对双口 RAM 进行检测，如图 4 所示。

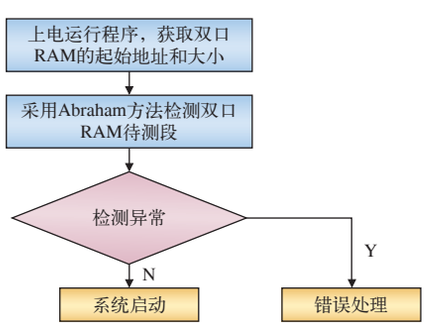

图4　双口RAM上电检测流程图

对双口 RAM 进行在线检测时，根据测试区的起始地址和区块大小，实时的利用内存检测算法对双口 RAM 进行功能性失效检测，如果发现故障，系统进行告警处理，流程如图 5 所示。

2.4 数据交互软硬件设计

在 MPU 和 HCU 中，通过设计依据角色轮换功能读写双口 RAM 的软件模块，完成双口 RAM 的访问操作。

双口 RAM 的 MPU 上软件交互关键代码如下：

```
switch(Start_Flag)
{
```

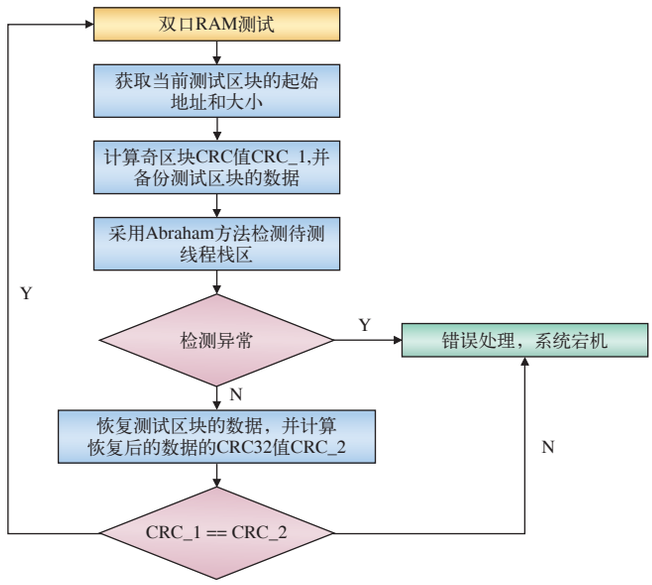

图5　双口RAM在线检测流程图

```
case 1:
        if(GM_FALSE == bMsgFalg)
        {
            Start_Flag = 0;
        }
        else
        {
            Start_Flag = 2;
        }
        break;
case 2:
        Get_Data_From_HCU(iBaseDevice);
        break;
case 3:
        Process_Vital_Data(iBaseDevice);
break;
case 4:
        Write_Data_To_HCU(iBaseDevice);
        break;
case 5:
        Start_To_Test(pChan,iBaseDevice);
        break;
case 6:
        DRAM_Role_Cycling(pChan,iBaseDe
vice);
```

```
            break;
        default:
            break;
        }
```

本文采用的 Abraham 算法检测时间与内存容量成线性关系，可以有效的控制检测时间，保证较高的检测速度，同时检测覆盖率也比较高，Abraham 算法性能参数如表 2 所示。

表2 Abraham算法性能参数

参数 / 内存段	测试算法	测试效率	覆盖率
双口RAM	Abraham	1 K (bit/ms)	99%

总体诊断覆盖率为 99%，可以满足铁路安全标准 EN50129[4] 中对大规模集成电路的测试方法和标准 IEC61508-2[5] 附录 A 中对安全相关硬件的随机失效的诊断覆盖率要求。

软件计算序列如下：

```
    /* Initialize */
    Abraham_Init(address,size,Pattern);
    /* sequence 1 */
    ret = Abraham_Sequence_1(address,size,Patter
n,AntiPattern);
    if(GM_FALSE == ret)
    {
        /* call fault manage function */
        return ret;
    }
    /* sequence 2 */
    ret = Abraham_Sequence_2(address,size,Patter
n,AntiPattern);
    if(GM_FALSE == ret)
    {
        /* call fault manage function */
        return ret;
    }
    /* sequence 3 */
    ret = Abraham_Sequence_3(address,size,Patter
n,AntiPattern);
    if(GM_FALSE == ret)
    {
        /* call fault manage function */
        return ret;
    }
    /* sequence 4 */
    ret = Abraham_Sequence_4(address,size,Patter
n,AntiPattern);
    if(GM_FALSE == ret)
    {
        /* call fault manage function */
        return ret;
    }
    /* sequence 5 */
    ret = Abraham_Sequence_5(address,size,Patter
n,AntiPattern);
    if(GM_FALSE == ret)
    {
        /* call fault manage function */
        return ret;
    }
    /* sequence 6 */
    ret = Abraham_Sequence_6(address,size,Patter
n,AntiPattern);
    if(GM_FALSE == ret)
    {
        /* call fault manage function */
        return ret;
    }
    /* Reset */
    Abraham_Reset(address,size,AntiPattern);
    /* sequence 7 */
    ret = Abraham_Sequence_7(address,size,Patter
n,AntiPattern);
    if(GM_FALSE == ret)
    {
        /* call fault manage function */
        return ret;
    }
```

（下转 P61）

显示实际运行速度，而列车运行进度控件显示列车当前位置。当点击常规制动按钮时，速度仪表盘的速度会迅速减小，速度指针逆时针方向转动；当点击紧急制动按钮时，速度仪表盘的速度会迅速变为 0，速度指针指向 0；点击制动缓解按钮时，速度仪表盘的速度恢复正常显示；当点击语音播报按钮时，列车到站时刻会自动播放音乐，列车启动后会自动停止播放音乐。

图5　系统运行状态2

5　结束语

本文对城市轨道交通列车司机驾驶控制台进行了模拟仿真，该系统为列控系统的研究提供一个模拟与仿真平台，有助于节省人力、物力资源，用于培训司机的正常操作和事故演习，保证铁路运营实施的安全性。

参考文献：

[1] 张国宝 . 城市轨道交通运营组织 [M]. 2 版 . 上海 : 上海科学技术出版社，2012.
[2] 郭北苑 . 高速列车驾驶界面人因适配性设计理论与方法研究 [D]. 北京 : 北京交通大学，2010.
[3] 李　洋 . 基于乘务员特性的机车驾驶界面优化设计研究 [D]. 成都 : 西南交通大学，2012.
[4] 唐　涛 . 列车运行控制系统 [M]. 北京 : 中国铁道出版社，2012 : 149-160.
[5] 孙　鑫 .VC++ 深入详解 [M]. 北京 : 电子工业出版社，2006 : 660-699.

责任编辑　徐侃春

（上接 P52）

```
/* sequence 8 */
ret = Abraham_Sequence_8(address,size,Patter
n,AntiPattern);
if(GM_FALSE == ret)
{
    /* call fault manage function */
    return ret;
}
```

主逻辑处理模块的一个逻辑处理周期内 600 ms，其中数据接收发送阶段 300 ms，写入区块或者读出区块的数据处理速率为 1 kbit /ms，有效交互时间 280 ms 内可以交互高达 280 kbit 的数据，可以满足系统的数据通信量。

在每个处理周期内，MPU 和 HCU 需要检测的双口 RAM 存储器区块都为 21 kbit，检测每个测试区块所用的时间为 21 ms。从以上性能可以看出，数据交互效率和双口 RAM 测试性能，可以同时满足系统的通信效率、故障检测覆盖率以及检测速度。

3　结束语

文章分析了应用在轨道交通行业中的实时安全设备的双口 RAM 数据通信要求，并在实际的项目设备开发中，设计了双 CPU 系统的安全数据交互方案，可以满足嵌入式安全设备数据交互的安全性和实时性要求。

参考文献：

[1] 燕　飞，唐　涛 . 轨道交通信号系统技术的发展和研究现状 [J]. 中国安全科学学报，2005，15（6）: 94-99.
[2] 姜　平，周荣根，肖红升，等 . 基于双口 RAM 的多机数据通信技术 [J]. 仪表技术与传感器，2005（15）: 105-107.
[3] 任爱玲，凌　明，吴光林，等 . 一种用于嵌入式内存测试的高效诊断算法 [J]. 应用科学学报，2005，23（2）: 178-182.
[4] CENELEC EN50129-2006. Railway Applications:Safety Related Electronic Systems for Signalling[S]. 2006.
[5] IEC61508-2. Functional Safety of Electrical/Electronic /Programmable Electronic Safety-related Systems-Part II[S]. 2010.

责任编辑　徐侃春