

文章编号: 1005-8451 (2015) 10-0047-04

计算机联锁中安全编码编程器的设计与实现

刘培顶, 陈荣武, 王黎敏, 陈 忱

(西南交通大学 信息科学与技术学院, 成都 610031)

摘 要: 在部分计算机联锁系统中, 输入和输出采用安全编码的方式来保证采集和驱动的安全性。安全编码需事先固化到安全输入/输出板的Flash存储器中, 输入/输出板通过读取安全编码的状态来判断系统是否正常工作。为此设计了使用C8051F020单片机作为控制器的编程器, 并基于Qt设计了上位机程序来实现对输入/输出板上28F128J3F75 Nor Flash的操作, 包括自动识别输入/输出板、读/写安全编码等。在文中详细介绍了系统结构、硬件连接、软件设计以及上位机读/写安全编码的数据格式定义。

关键词: 计算机联锁; 安全编码; C8051F020; 28F128J3F75; Qt

中图分类号: U284.3 : TP39 **文献标识码:** A

Secure coding programmer for Computer-based Interlocking System

LIU Peiding, CHEN Rongwu, WANG Limin, CHEN Chen

(School of Information Science and Technology, Southwest Jiaotong University, Chengdu 610031, China)

Abstract: In some kinds of Computer-based Interlocking System, secure coding was used for input and output to guarantee the safety of acquisition and driving. Secure coding should be programmed into the safety input/output board's Flash memory previously. According to the state of security coding, the input/output board determined whether the system worked properly. The paper designed a programmer which used 80C51F020 single-chip microcomputer as its controller, and also designed the PC program based on Qt to implement the operation of 28F128J3F75 Nor Flash chip, including input / output board of automatic identification, read / write secure coding, etc. It was described the system architecture, hardware connections, software design and the data format definition of PC program reading or writing secure coding in detail.

Key words: computer-based interlocking; secure coding; C8051F020; 28F128J3F75; Qt

计算机联锁系统在保障行车安全上起着至关重要的作用, 必须符合“故障—安全”原则。为确保联锁机与监控对象之间信息的传送安全, 在通道设计上须采用安全输入/输出接口, 通常采用光电隔离技术、安全编码以及表决来实现。在光耦输入端施加特定的安全编码信号, 在另一光耦输出端对信号进行回采, 若输出与预期不符, 则表明有故障, 由安全电源控制板控制安全重力继电器切断输出电源, 实现故障导向安全。每一路对应的安全编码应事先固化到安全输入/输出板的板载Flash存储器中, 出于安全考虑, 系统在启动后只能在线读取Flash中的编码, 而不能擦写Flash, 即不支持在线编程, 这就需要有一个离线编程器专门给安全输入/输出板进行编码。该编程器设计的好坏, 直接关乎联锁系统安全

编码的正确率和以后的工程配置效率。

1 芯片选型及性能介绍

为了提高计算机联锁系统可靠性和随机读取速度, 安全地输入/输出板上的Flash存储器采用Intel公司的28F128J3F75 Nor Flash。为了减少系统功耗并缩短开发周期, 设计了一种以C8051F020高性能单片机为主控制器的编程器, 并基于Qt设计了上位机程序, 通过RS232串口通信来控制编程板对Flash存储器实现读、写、擦除等操作。

1.1 Flash芯片28F128J3F75

根据编码理论, 利用 n 位二值码元可生成 2^n 种状态的码字或代码的集合。在这 2^n 种状态的代码组合中, 仅有一种状态代表危险侧码字, 其余均为安全侧码字。在铁标《TB/T 3027-2002 计算机联锁技术条件》中规定:

收稿日期: 2015-01-24

作者简介: 刘培顶, 在读硕士研究生; 陈荣武, 高级工程师。

(1) 有相同意义的与行车安全有关的变量及其同一变量不同取值的信息编码的汉明码距应不小于4；

(2) 与行车安全有关的信息编码，在其码集中合法码字、非法码字或安全侧码字和非安全侧码字的不对称比率必须不小于255:1^[1]。故在设计安全编码时，码位至少为8，从安全冗余以及方便软件编程的角度出发，通常设计为16 bit或32 bit。经过正确的合理编码，完全可以保证编码的汉明距大于4^[2]。

基于以上原因，联锁系统中，安全输入/输出板上的Flash存储器一般采用16 bit I/O口的Flash芯片。安全编码从16 bit变为32 bit时，使用2片Flash，增加片选信号线，分时对Flash进行操作。本设计针对的安全输入/输出板上，Flash存储器为28F128J3F75 Nor Flash芯片，芯片采用分块结构，非常适合于要求高密度的代码或者数据存储的低功耗系统。它具有以下特点：

(1) 速度快：异步页模式读取25 ns/8 word；在256 byte缓冲器写模式下有效编程时间为1.41 us。

(2) 低功耗：其供电电压为2.7 V~3.6 V，根据手册擦写功耗最大为80 mA×3.3 V。

(3) 具有通用Flash接口，用户可根据需要配置为x8或者x16模式；具有128个128 kbyte/64 kWord的可擦除块，该特性允许用户对其中任意一个块数据进行擦除或者编程。

(4) 可靠性高：工作温度为-40℃~+85℃；V_{pp}=GND时可实现完全写保护，具有灵活的块上锁，电压跳变时可中止擦除/写入操作；每块循环擦写次数为10万次以上。

1.2 编程器主控制器C8051F020

编程板设计时采用5 V的USB接口供电，考虑到一般计算机USB口供电能力为300 mA左右，所以元器件选择以及设计时需要考虑降低功耗。安全输入/输出板编程时主要功耗为FLASH，根据28F128J3F75数据手册，3.3 V供电电压下，其擦写功耗最大为80 mA。其它板载电路如CPCI和逻辑控制电路等都处于待机状态，功耗可以估计为10 mA左右，即在编程时安全输入/输出板最大电流为90 mA，功耗约为300 mW，在设计编程板上电路时总功耗尽量保持在1.2 W以内。考虑到以上原因，同

时为了方便系统开发，在设计时采用C8051F020芯片作为编程器主控制器。

C8051F020是完全集成的混合信号系统级芯片(SoC)，具有功能全面、应用广泛、性价比高等优点。它具有与8051兼容的CIP-51微控制器内核，指令系统完全相同，熟悉MCS-51系列单片机的工程技术人员可以很容易地掌握C8051F^[3]。与Flash安全编码相关的特性如下：

(1) 采用流水线结构，与标准的8051结构相比指令执行速度提高了大约10倍；最大系统时钟频率为25 MHz，峰值速度达到25 MIPS。

(2) 拥有8个8 bit的I/O端口，大量地减少了外部连线和器件扩展，有利于提高可靠性和抗干扰能力。

(3) 工作电压为2.7 V~3.6 V，与Flash工作电压兼容；支持多种节点休眠和停机方式，每个端口I/O引脚都可以被配置为推挽或漏极开路输出，在标准8051中固定的“弱上拉”可以被总体禁止，这为低功耗应用提供了进一步节电的能力。

(4) 自带4 K XRAM，读/写Flash时可提供足够大的数据缓冲区。

(5) 支持JTAG调试和边界扫描，可以进行非侵入式、全速的在系统调试^[4]。

2 系统结构及硬件接口设计

近年来新开发的计算机联锁硬件平台均采用CPCI总线，因此设计编程板时要加入CPCI接口。编程板由5 V USB供电，通过CPCI接口与安全输入/输出板的J2口相连，上位机通过RS232接口与编程板进行串口通信，发送读、写、擦除等命令，控制编程板上的主控制器C8051F020单片机对安全输入/输出板上的Flash芯片执行相应的操作。JTAG接口用于烧写程序至单片机，并提供在线调试。在编程板上设计有状态灯，用于显示电源和工作状态。系统结构如图1所示。

C8051F020有8个8 bit的I/O端口，低端口(P0、P1、P2和P3)既可以按位寻址也可以按字节寻址，除作通用I/O口外，可作为其他功能模块的输入输出引脚，通过交叉开关配置器选择并控制。高端口(P4、

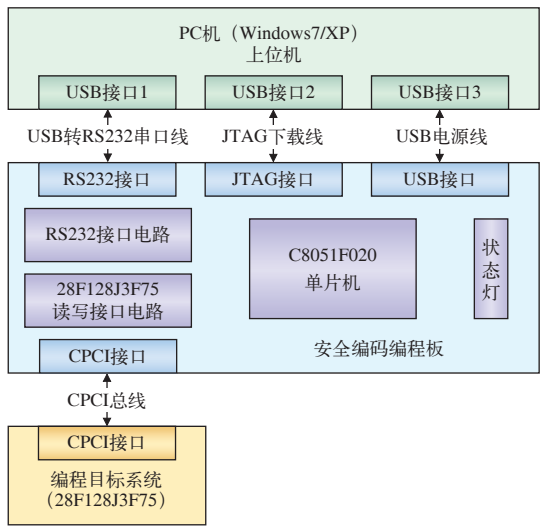


图1 安全编码编程器的系统结构

P5、P6 和 P7）只能按字节寻址^[4]。根据交叉开关译码表，P0.0 和 P0.1 脚分别作为串口通信的 TX0 和 RX0，并且位置不能互换。在硬件电路设计时，为充分利用单片机 I/O 口，P0.2~P0.7 作为 Flash 芯片的控制线，控制片选信号（P0.2、P0.3 分别控制两块 Flash 芯片的 CE0 片选信号，实现 32 bit 编码）、写保护、复位信号、读使能、写使能，P1 预留，P3、P2 作为数据线，与 Flash 的 DQ15~DQ0 相连，P6、P5、P4 作为地址线，与 Flash 的 A24~A1 相连，P7 接状态灯。由于采用 16 bit 数据位，因此 Flash 芯片上的 BYTE 接 VCC，硬件置 1，A0 接地。在此，给出 C8051F020 与 28F128J3F75 相关部分连接图，如图 2 所示。

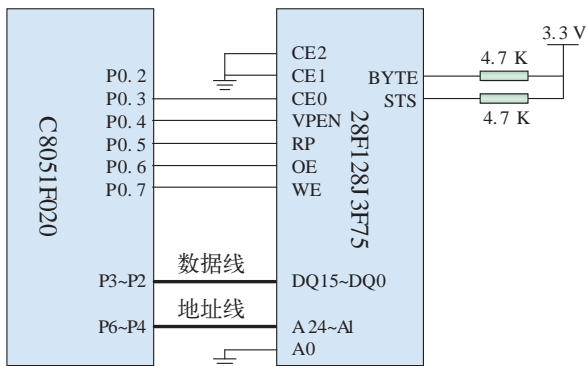


图2 C8051F020与28F128J3F75硬件接口电路

3 软件设计

软件设计时，为了程序的可移植性和易用性，

将程序分为 3 个层次。第 1 层是硬件抽象层，第 2 层是实现访问 Flash 的命令层，第 3 层是应用层，提供给用户或文件系统的接口函数。

3.1 硬件抽象层

硬件抽象层包括访问 Flash 的硬件环境配置以及单片机与 Flash 接口实现通讯的基本函数。硬件环境配置包括 C8051F020 系统时钟初始化、I/O 端口配置、串口初始化、Flash 芯片初始化。与 Flash 接口实现通信的基本函数即为 Flash 的读 / 写函数：从给定的 24 bit 地址，读取一个字的数据，或往该地址写一个字的数据或命令。对 Flash 芯片的所有操作均基于这两个函数。C8051F020 是 8 bit 的系统，而读 / 写 Flash 时数据线的为 16 bit，地址线为 24 bit。为了提高程序运行效率，避免地址操作时的溢出和进位判断，定义了一个 unsigned long 型变量 F_Addr 表示地址（C8015 中为 32 bit），设置宏定义，通过指针和取地址的方式，取其低 24 bit 分成 3 个 8 bit 分别赋值给 C8051F020 的 P6~P4 口，如下所示：

```
#define h_long(x) (*((unsigned char *)&x+1))
#define m_long(x) (*((unsigned char *)&x+2))
#define l_long(x) (*((unsigned char *)&x+3))
```

经测试，使用该方式读取 Flash 数据的效率高干定义全局变量或使用移位操作符赋值的方式。通过研究 28F128J3F75 芯片数据手册中的单字异步读时序图和异步写时序图，使用 _nop() 指令延时及控制读 / 写信号、片选信号电平高低来模拟 Flash 的读 / 写时序，即可封装成最基本的读 / 写函数 void Flash_WR(unsigned long F_Addr, unsigned int Data_h, unsigned int Data_l)、int Flash_RD (unsigned long F_Addr) 供命令层函数使用。其中，Data_h、Data_l 分别表示数据的高 8 bit 和低 8 bit 赋给单片机的 P3 口和 P2 口。

3.2 命令层

调用硬件抽象层的基本读 / 写函数生成 Flash 的命令函数，包括读取状态寄存器状态、清除状态寄存器状态、CFI 查询、读 Flash 芯片 ID 号和设备号、按块擦除、按字写、缓冲器写、读阵列等。在 Flash 芯片数据手册中，每一个命令操作均有详细的流程图供开发者参考使用。

3.3 应用层

提供用户程序访问 Flash 的高级接口函数，包括写安全编码、读安全编码、自动识别安全输入 / 输出板、擦除整块 Flash 芯片等函数。用户不需要知道 Flash 的内部结构和接口协议，单片机所有初始化完毕后即进入 while(1) 循环,等待用户程序发来的命令，进而执行相应的操作。

4 上位机及数据格式定义

在工程应用中，安全编码一般以十六进制存放于 .dat 文件中，为了方便读 / 写安全编码，基于 Qt 软件设计了上位机程序，其界面如图 3 所示。除具有串口助手的基本功能外，增加了许多安全编码编程器相关的功能，包括加载 .dat 文件、读 Flash 信息、擦除 Flash 芯片、烧写安全编码数据、读安全编码数据、数据管理等。

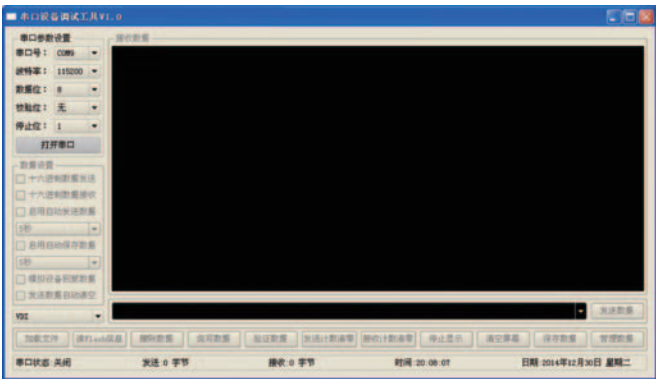


图3 编程器上位机程序界面

上位机与编程器之间使用 RS232 串口通信，C8051F020 单片机使用 UART0 的方式一，即异步工作，8 bit 数据位，一个起始位，一个停止位。

安全编码使用大端存储方式，即数据的低字节存放在内存的高地址，数据的高字节存放在内存的低地址。读 / 写安全编码时均按此种方式。

读 / 写安全编码时，以 1 kbyte 数据为单位进行读 / 写，为保障安全性，数据格式定义如表 1 所示。

表1 读/写安全编码数据格式

数据定义	编号N	安全编码数据	校验值
数据长度	2 byte	1 kbyte	2 byte

Flash 芯片基地址定义为 0x000000，上位机写数据时，编程板根据编号值来确定安全编码数据的存

储位置；上位机读数据时，编程板根据地址计算编号值。安全编码为 16 bit 时，F_addr=512 N，安全编码为 32 bit 时，F_addr=256 N。校验值采用最简单实用的方式，即将编号 N 与安全编码数据共 1 002 byte 的数据累加。上位机与编程板均需要计算校验值，将收到的校验值与计算的校验值进行比较，若相等则表明收到的数据是正确的，执行相应的读 / 写操作；若不相等，则显示警告信息，并在编程板上以流水灯的形式表现，提示用户数据有误，中断读 / 写操作。

5 结束语

在输入 / 输出采用安全编码的联锁系统中，安全编码编程器的设计必须要有非常高的安全性和可靠性。通过认真分析功能需求及电气技术要求，设计了以 C8051F020 为主控制器的编程器及上位机程序。编程器设计紧凑，轻便小巧，使用一台笔记本即可进行测试与调试。在 115 200 波特率下，安全编码读、写速度分别为 7 kbyte/s、3 kbyte/s，完全满足工程应用需求。目前整套系统已应用于国内某自主研发的计算机联锁系统硬件平台中。

参考文献:

[1] 中华人民共和国铁道部. TB/T 3027-2002. 计算机联锁技术条件 [S]. 北京: 中国铁道出版社, 2002.

[2] 陈学伍, 陈洪亮. 数据库原理与工程应用 [M]. 合肥: 中国科学技术大学出版社, 1996.

[3] 孙立香, 赵不贿, 刘星桥. C8051F020 与 80C51 单片机的异同点 [J]. 国外电子元器件, 2007 (5): 31-35.

[4] 潘琢金, 施国君. C8051Fxxx 高速 SoC 单片机原理及应用 [M]. 北京: 北京航空航天大学出版社, 2002.

[5] 李长有, 武学东, 孙步胜, 马齐爽. 基于 C8051F020 的 SD 卡主控制器设计 [J]. 微计算机信息, 2007 (26): 120-122.

责任编辑 徐侃春

