目录

[一、功能描述 2](#_Toc10152)

[二、设计方案 2](#_Toc10554)

[三、安全设计描述 3](#_Toc4646)

[1. 抗攻击设计-执行冗余 3](#_Toc15143)

[2. 容错设计-阻塞设计、超时处理设计 3](#_Toc20164)

[3. 抗干扰设计-输入滤波 3](#_Toc31297)

[4. 抗攻击设计-控制冗余 4](#_Toc20031)

[5. 容错设计-数据校验 4](#_Toc29332)

[四、 软件设计 4](#_Toc31124)

[1. 抗攻击设计-执行冗余 4](#_Toc18889)

[2. 容错设计-阻塞设计、超时处理设计 5](#_Toc9724)

[3. 抗干扰设计-输入滤波 5](#_Toc30107)

[4. 抗攻击设计-控制冗余 6](#_Toc14857)

[5. 容错设计-数据校验 6](#_Toc29456)

[6. 操作流程 7](#_Toc5238)

[五、设计总结 8](#_Toc27776)

# 一、功能描述

编写程序，实现FS-STM32F407 开发平台上的直流电机的正反转实验。调试编译好固件程序后，将程序下载到FS-STM32F407 开发板。

用户可以按下开发平台的1，2，3实现不同速度的正转，4，5，6实现不同速度的反转。转速将通过数码管显示。

程序设计过程中运用了嵌入式安全设计的思想，包括抗干扰设计，容错设计，抗攻击设计三个方面。

# 二、设计方案

在课程给出的例程3\_DC\_MOTOR的基础上修改，添加抗干扰设计，容错设计，抗攻击设计。

3\_DC\_MOTOR原本功能为：按下1、2、3中的任意一个键，风扇正转；按下4、5、6中的任意一个键，风扇反转；按下其他键，风扇停止转动。同时通过数码管显示风扇转速。

修改后，需要连续按下8次按键，滤波后选择合适的输入用于设置风扇转速。

同时在程序运行过程中添加随机延时、序列检查、数据校验等安全设计，详见安全设计描述。若符合安全设计，则程序正常运行，外在表现的功能与基础功能相同，否则会报错。

# 三、安全设计描述

## 1. 抗攻击设计-执行冗余

① 在程序中插入一些随机时延（random sleep），使得程序段的运行时间不固定。使得攻击者无法根据程序段运行时间发现内部信息，进行旁路攻击。

## 2. 容错设计-阻塞设计、超时处理设计

① 阻塞设计。设置变量flag。当flag为1允许输入、数据处理、输出，否则程序循环等待。使得程序只在允许的时间范围内进行指定的操作。

② 防止超时设计。上述阻塞设计可能导致程序等待时间过长；此外其他的意外、错误也可能导致程序超时。故添加变量cnt。初始化为0，不断递增。每次正常执行完毕都会清零。若cnt数值过大，说明超时。

## 抗干扰设计-输入滤波

① 输入滤波。连续读取8次输入。取这8次输入中出现最多的输入（若两个输入出现次数相同，取最新的输入），并判断其出现次数是否超过8次的一半。若超过，则认为输入正常，取该输入继续进行其他处理。否则认为输入出错。

这里由于输入按键不会清零(按键时间间隔为几十毫秒,读数时间间隔只有几毫秒)应该是读取同一个输入8次，也可能由于新的输入/其他干扰导致变化。为了防止这些干扰，添加此输入滤波。

## 4. 抗攻击设计-控制冗余

① 序列检查。设置变量judge，用于标记代码块块号，并检查。正常的程序执行应该是按照一定的代码块顺序的，而攻击者有可能跳过一些代码块直接执行之前/之后的关键代码。为了防止这种攻击，添加序列检查。

举例：执行第3块代码块时，先检查judge是否为2，若是，则说明刚刚执行了第2块代码块，则第3块代码块正常执行，执行结束后修改judge为3.若judge判断出错，说明程序执行序列有问题，出错。

## 5. 容错设计-数据校验

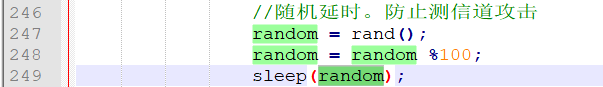
① 对输入及送到串口处理的数据采取CRC校验。首先利用确认好的输入数据生成CRC校验码，当送往串口处理后，利用刚刚生成的校验码进行校验。这样可以防止从输入到送往串口处理的过程中发生数据的干扰、变化。

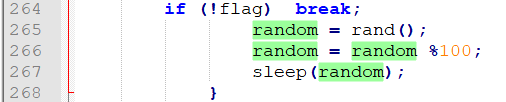
# 软件设计

以下代码均为工程文件/Src文件夹/main.c中的代码。

## 1. 抗攻击设计-执行冗余

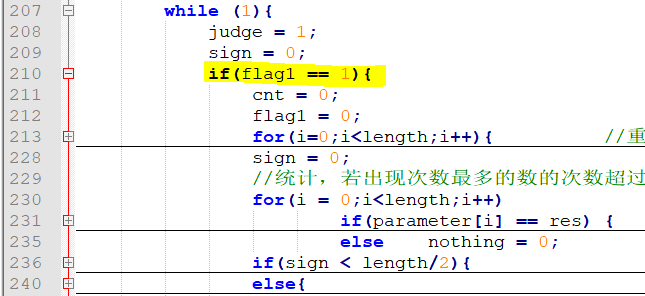
① 在程序中插入一些随机时延（random sleep）.



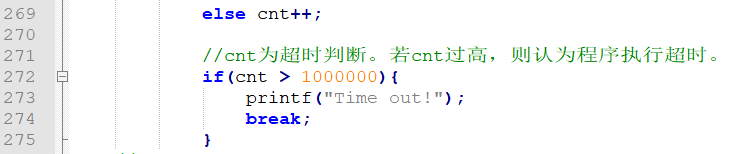


## 容错设计-阻塞设计、超时处理设计

① 阻塞设计。见标黄的flag1

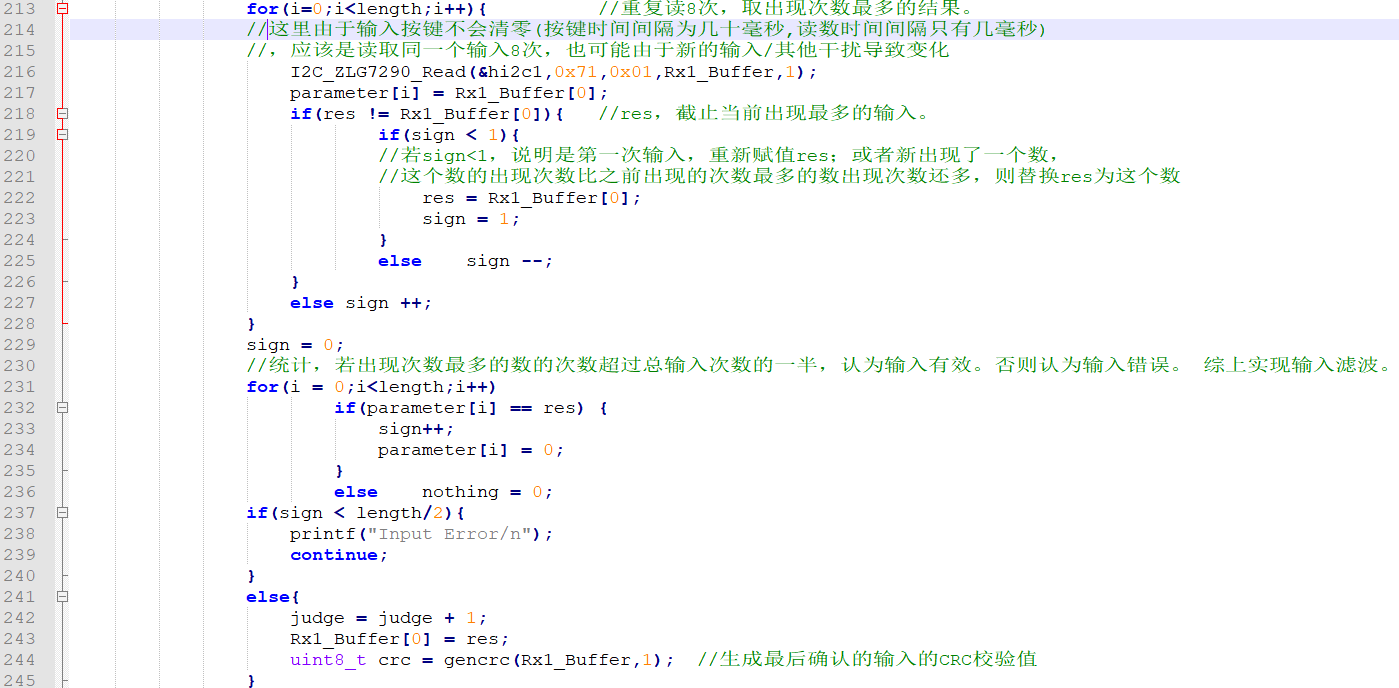


② 防止超时设计。



## 抗干扰设计-输入滤波

1. 输入滤波。

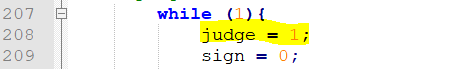


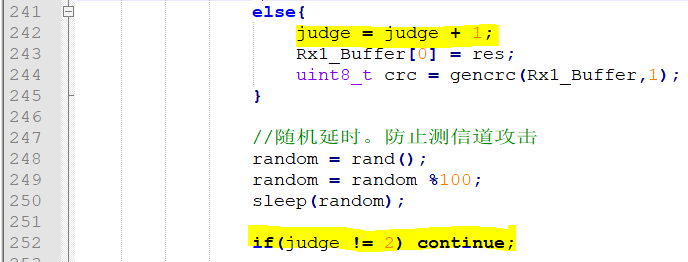
## 4. 抗攻击设计-控制冗余

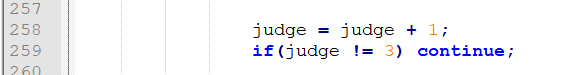
① 序列检查。见judge的赋值以及if判断





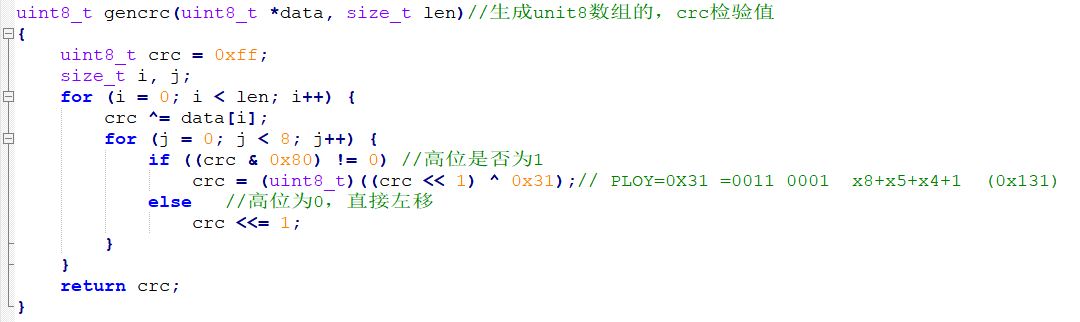


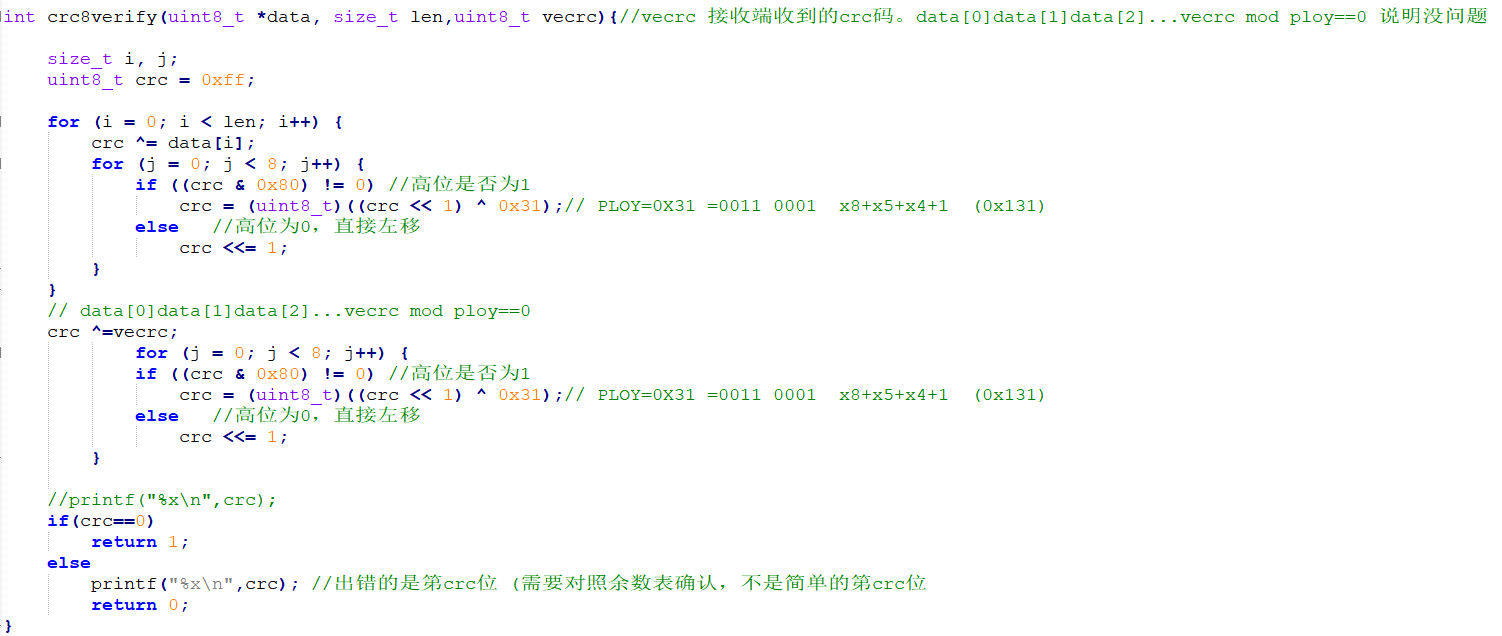


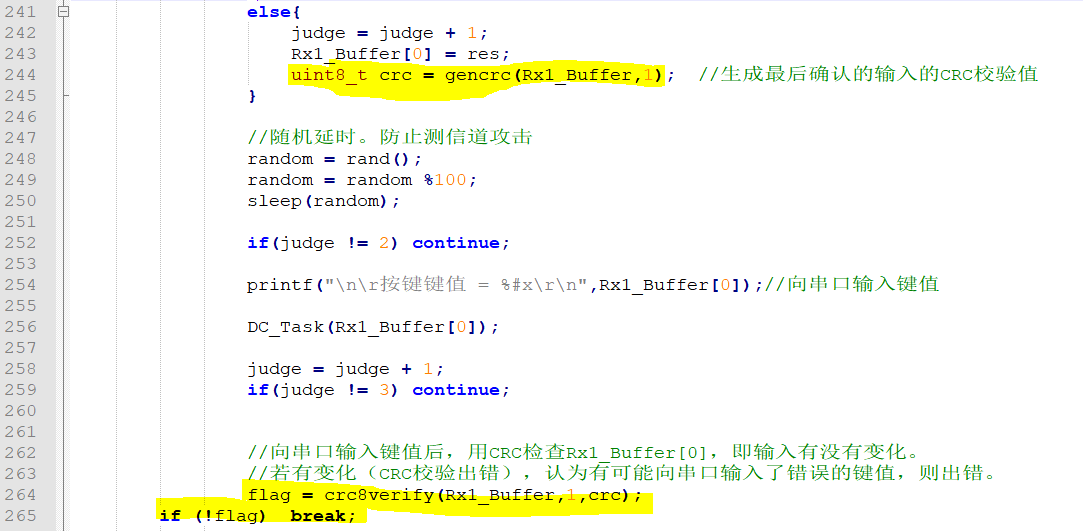


## 5. 容错设计-数据校验

① 对输入及送到串口处理的数据采取CRC校验。



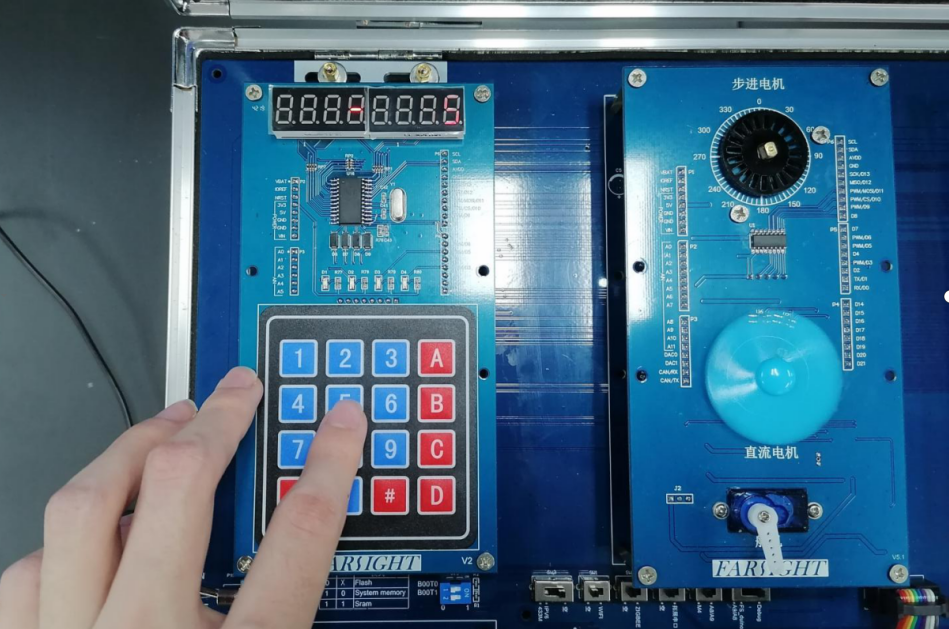




## 操作流程

将工程下载到开发板上，按下1，2，3，风扇以不同风速正转，数码管显示正转速。按下4，5，6风扇以不同风速反转，数码管显示负转速。实验效果如下：

按下5反转：



正转

