基于 STM32F105 微控制器的双 CAN 冗余设计方案

控制器局域网（ ControllerA reaN etwork， CAN）是一种多主方式的串行通讯总线。CAN 总线具有较高的位速率， 很强的抗电磁干扰性， 完善的错误检测机制， 在汽车、制造业以及航空工业领域中得到广泛应用 。由于船舶机舱环境极为恶劣， 且船舶航行过程中维修条件不如陆上， 对 CAN 通信的可靠性要求很高， 采取双 CAN 冗余总线提高通信可靠性。本文提出一种基于 STM32F105 微控制器的双 CAN 冗余设计方案。

1 硬件平台组成

STM32F105 是 STM icroe lectron ics 公司推出的一款基于 ARM Cortex- M3 内核的 32 位微控制器， 其内核是专门设计于满足高性能、低功耗、实时应用的嵌入式领域的要求。由于采用 Thumb - 2 指令集，与 ARM7 微控制器相比 STM32 运行速度最多可快 35% 且代码最多节省 45% 。较高的主频和代码执行效率使系统在进行 CAN 总线数据收发的同时仍可运行总线冗余算法。STM32F105 微控制器内部集成 2 路独立的 CAN 控制器， 控制器集成在芯片内部， 避免了总线外扩引入的干扰， 同时简化了电路设计、降低成本。

系统使用两条完全独立的 CAN 总线， 两个 CAN 总线收发器和总线控制器，实现物理层、数据链路层的全面冗余。在初始化时两个控制器被同时激活， 一个作为主 CAN， 另一个作为从 CAN， 为主控制器的备份。正常运作时， 数据通过主 CAN 优先发送； 当主 CAN 总线繁忙时， 从 CAN 总线分担部分通信流量；而当主 CAN 总线发生故障时， 数据转移至从 CAN 控制器传输， 反之亦然。在任一总线发生故障时，数据都能经由另一条总线传输，而当两条总线都正常时，使用两总线同时传输， 增加约 1 倍的通信带宽，这样在保证了通信可靠性的同时提高了实时性。

CAN 总线接口电路设计如图 1 所示， 使用 T JA1050 作为总线收发器， 它完成 CAN 控制器与物理总线之间的电平转换和差动收发。尽管 TJA1050 本身具备一定的保护能力，但其与总线接口部分还是采用一定的安全和抗干扰措施；TJA1050 的 CANH 和 CANL 与地之间并联两只 10pF 的小电容， 可以滤除总线上的高频干扰； 另外， 为了增强 CAN 总线节点的抗干扰能力， 总线输入端与地之间分别接入一只瞬态抑制二极管， 当两输入与地之间出现瞬变干扰时， 收发器输入端电压被钳位在安全范围。

为防止总线过压造成节点损坏， STM32F105 内置 CAN 控制器的数据收发引脚并不与 TJA1050 直接相连， 通过 ADuM1201 磁隔离器实现信号隔离传输。与传统光耦隔离相比， 磁隔离简化了隔离电路设计， 并且磁隔离芯片的功耗很低，大约相当于光耦隔离的 1 /10。除了将 CAN 数据信号隔离外，TJA1050T 使用的

电源和地也必须与系统完全隔离， 使用 5V 隔离输出的开关电源模块 IB0505LS 提供隔离电源。由于 CAN 总线数据传输率较高， 为了提高信号质量， 网络拓扑结构应尽量设计成单线结构以避免信号反射， 同时终端连接 120 欧姆左右的匹配电阻。

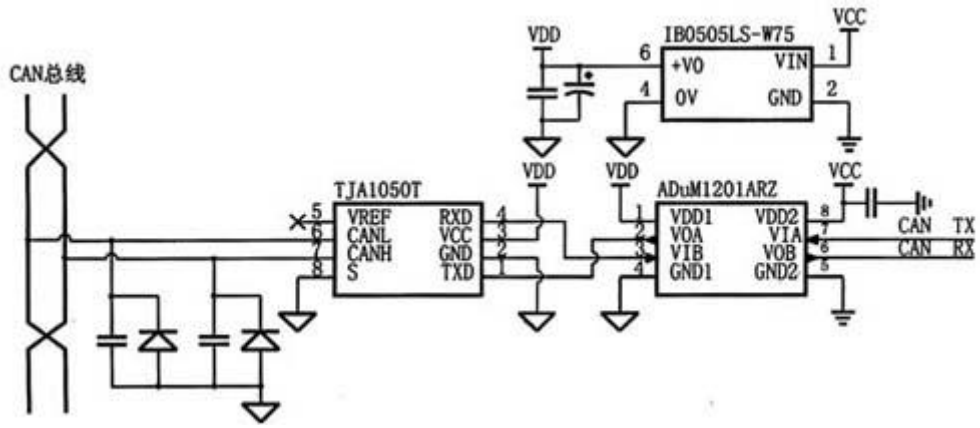

图 1 CAN 接口电路设计

2 软件设计

CAN 协议规范定义的数据链路层和部分物理层并不完整， 双 CAN 冗余应用需要实现总线状态监控、网络故障的诊断和标识， 这就要通过添加软件冗余模块来实现。冗余模块在程序主循环中调用， 根据不同总线错误状态执行收发通道切换。CAN 总线错误状态分为 3 类： 错误激活、错误认可、总线关闭。总线正常工作时处于错误激活状态，控制器检测到错误后将发送/接收错误计数器的值递增， 当值大于 127 时进入错误认可， 大于 255 时总线关闭状态， CAN 总线错误检测模块通过读取错误状态寄存器作为总线故障的测试条件， 在错误状态发生改变时调用冗余算法， 执行总线切换操作。

通过实际调试发现， 总线连接断开且只有 1 个节点不断发送报文时产生发送错误， 控制器进入错误认可状态， 但不进入总线关闭状态； 其它错误均使错误计数器增加， 依次进入错误认可状态、总线关闭状态， 后两种状态表明总线被严重干扰， 需要采取相应措施。为简化控制逻辑设计将错误认可和总线关闭合并为总线故障。

冗余算法使用状态机实现发送模式的切换， 根据不同总线故障选择发送使用的总线。状态切换流程图如图 2 所示， 程序首先读取错误状态寄存器获得总线错误状态， 判断当前总线是否处于错误激活模式， 若检测到总线故障程序置

相应标志位向其他程序模块指示错误。为提高报文发送效率， 发送程序一次将多个报文写入发送邮箱由硬件控制自动发送， 在切换总线时， 需先把故障总线发送邮箱中的报文中回读， 通过备份总线优先发送， 这一机制保证报文不会因总线切换而丢失。控制器向故障总线发送数据域为空的测试报文， 每成功发送 1 报文， 总线发送错误计数器的值递减， 直至其值小于 128 总线恢复到错误被动状态； 每隔一定时间冗余程序读取错误状态寄存器， 检测故障总线是否恢复正常。

在 2 总线同时传输模式， 发送程序优先写入总线 1 邮箱， 当总线 1 邮箱满时写入总线 2 的邮箱， 由于报文按优先级仲裁发送， 若某一路发送邮箱经常为空， 说明该路总线通信流量较小， 发送程序将较多报文转由空闲总线发送， 实现报文的负载均衡。

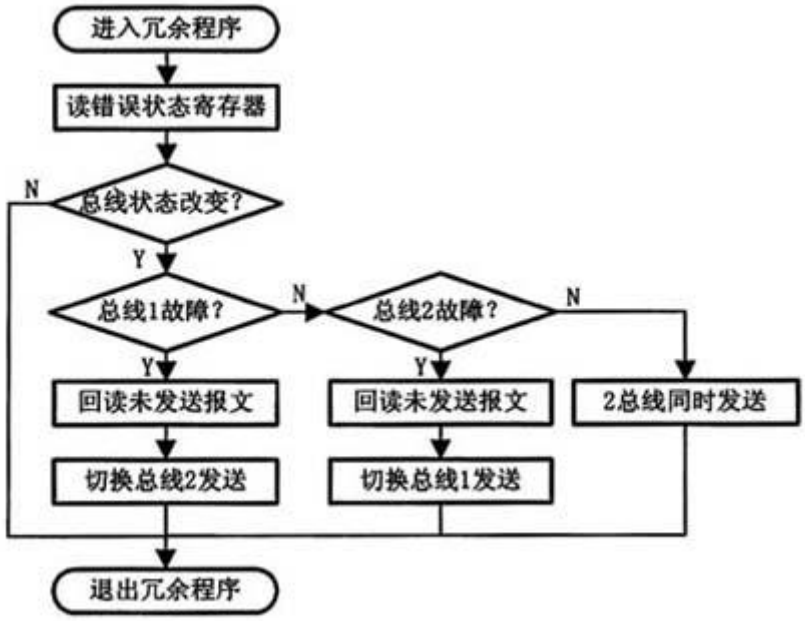

图 2 总线状态切换流程图。

3 双总线冗余的可靠性分析与测试

对双 CAN 冗余系统的可靠性进行定量分析， 引入平均无故障运行时间（M ean T ime To Fa ilure， MTTF）的概念。MTTF 描述一个系统从开始工作到发

生故障的时间间隔， 也即平均寿命。为简化分析作如下假设： 每路 CAN 总线的故障率相同； CAN 总线的损坏属于物理损坏， 即不可修复的损坏。指数分布可以很好地用来描述电子元器件的寿命，假设 CAN 总线的寿命分布服从指数分布，CAN 总线的可靠性模型如图 3 所示。

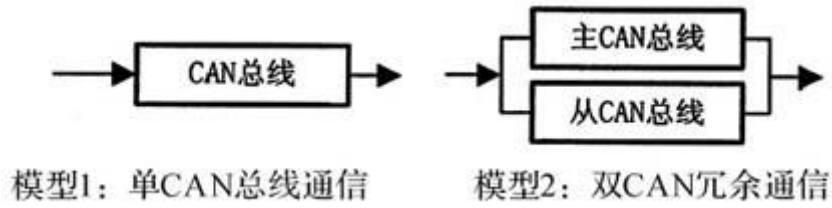

图 3 CAN 总线可靠性模型图

模型 1 为单总线的可靠性模型， 因为总线寿命服从指数分布， 根据单一 CAN 总线无故障运行时间 MTTF1 = 1 /λ 。模型 2 为双 CAN 总线冗余可靠性模型，系统由两条独立的总线并联而成， 即只有当这 2 条总线都失效时系统通信才会失败， 于是系统的平均寿命 MTTF2 = 3 /2。采用双线冗余设计使 CAN 通信的平均无故障时间增加了 50%。

双线 CAN 冗余系统的另一关键指标是总线切换时间， 它等于检测错误所需时间与处理故障总线未发送报文所需时间之和， 切换时间越短， 总线故障对报文传输造成的延迟就越小。检测错误所需时间，即从总线错误出现到被冗余程序检测到所需的时间。以总线断开故障为例， 发送器每发送一个报文产生一次应答错误， 错误计数器每次加 8， 需连续进行 16 次发送， 使错误计数器值达到 128 引起总线切换。在位速率 125kbps 情况下， 发送最长为 128 位的报文， 若忽略控制器重发间隔时间， 从故障发生到被检测到的响应时间为：

$$t_{REQ} = \frac{1}{125} \times 128 \times 16 = 16.38(ms)$$

为避免在总线切换时丢失报文，冗余算法需回读故障控制器中未发送报文，由此产生额外的故障处理时间， 因为每个发送邮箱最多存储 3 个报文， 假定位速率 125kbps 不变， 备份总线发送时即取得仲裁，最长故障处理时间为：

$$t_{HANDLE} = \frac{1}{125} \times 128 \times 3 = 3.07(ms)$$

因此总线切换时间为 16. 38+ 3. 07= 19. 45m s。

通过实验测得在 125kbps 位速率下连续发送不同报文长度的总线切换时间如表 1 所示：

表 1 总线切换时间

数据域长度(字节)	报文长度(位)	总线切换时间(ms)
0	64	14.00
1	72	14.80
2	80	16.00
4	96	18.40
8	128	22.80

在 125kbps 位速率下切换时间为 22. 80ms， 比理论计算值稍长， 这是由总线切换时运行冗余算法及读取控制器错误寄存器（ ESR）所额外消耗的， 但在实际应用中， 发送报文获取仲裁所需的等待时间远大于切换时间， 总线故障并不频繁发生， 冗余切换算法对系统的运行并无显着影响。

4 结束语

与传统单片机总线外扩两片 CAN 控制器的冗余方案相比， 本设计充分利用 STM32F105 微控制器内置的两路 CAN 控制器，简化电路设计，相对降低了成本，同时双 CAN 冗余通信系统的采用提高了系统整体可靠性。所使用双总线负载均衡技术， 可以提高总线带宽， 平衡通信负荷。系统船舶机舱监控系统的图像和数据信号的传输中取得很好的效果。