自适应前照灯转向系统的高可靠性设计

张紫瑞[1],严 锐[2],岳继光[1],吴继伟[1]
(1.同济大学 电子与信息工程学院,上海 201804;
2.浙江嘉利工业有限公司,浙江 丽水 323000)

摘 要:针对汽车自适应前照灯系统(AFS),分别从硬件设计和软件设计两方面进行了可靠性论述,并通过软硬件协同工作来提高系统整体可靠性;设计了两路主从冗余控制,并分析了系统的可靠性。

关键词:实时系统;高可靠性;冗余;AFS
中图分类号:TP302 **文献标识码**:A **文章编号**:1674-7720(2010)12-0101-03

Adaptive headlamps steering system design with high reliability

ZHANG Zi Rui[1], YAN Rui[2], YUE Ji Guang[2], WU Ji Wei[1]
(1.College of Electronic and Information Engineering, Tongji University, Shanghai 201804, China;
2.Zhejiang Jiali Industry Co.,Ltd., Lishui 323000, China)

Abstract: Considering the problems of the dependability for embedded software and hardware used in AFS, the methods to implementation dependability were discussed on two aspects. One aspect was the design of hardware, and another was the software design. Through the hardware and software collaborative work to improved overall system reliability, this paper also analysed the reliability of the system.

Key words: real-time system; high reliability; redundancy; AFS

实时系统(Real Time System)是指计算和动作方面具有性能期限的系统。实时系统一般是嵌入式的[1]。一方面,系统工作环境恶劣,受电噪声干扰影响较大;另一方面,由于软件复杂度高,导致系统运行稳定性问题日益严峻,故可靠性成为影响嵌入式系统优劣的重要因素[2]。随着微电子技术在汽车领域的应用越来越广泛,近几年的统计表明控制系统的硬件故障在不断减少,而软件系统的故障率却在快速上升[3]。但是软件以硬件为基础,如果能以可靠硬件为基础设计可靠的软件,便会大大提升系统运行时的可靠性,从而降低事故发生概率,达到保护生命和财产的目的。

现有AFS系统设计者只是单纯地针对系统的功能而设计,或者只是单纯地从软件上考虑容错性,很少有能从软硬件两方面设计可靠的嵌入式系统,尤其各种软硬件故障,都需要软件来充分挖掘、利用硬件资源进行容错设计,完成故障诊断和必要的纠正措施[4]。所以更好的、更可靠的实时系统应该从软硬件两方面去考虑,使软硬件协同工作,以实现更安全、更高效的工作。

本文针对汽车自适应前照灯转向系统开发中的可靠性设计问题,从硬件和软件两个方面进行讨论,在冗余硬件资源的基础上实现了算法冗余,并对系统的可靠性进行了详细的分析和评估。

1 AFS系统体系结构

AFS系统是一种自适应的车灯随动转向系统,可提高汽车夜间行驶在岔口、弯道处的可视性能,能够有效地降低驾驶者的疲劳程度,并且能够在驾驶者发现前方危险情况下延长驾驶者的反应时间。从而有效地降低夜间行车事故发生的概率。所以如果这种系统发生故障将会造成财产的损失甚至危及生命。系统的总体结构如图1所示。

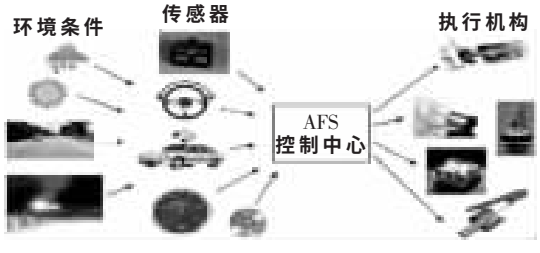

图1 AFS系统总体结构

AFS 系统中各路传感器采集天气条件、光强、方向盘转角、车速、车身变化等信号，经由车身网络到达 AFS 控制中心；在 AFS 控制中心进行优化组合，并采用合适的控制算法运算出车灯转向角，作用于执行步进电机，以完成车灯的自适应转向。

2 硬件可靠性设计

硬件是软件设计的基础，可靠的硬件设计为系统整体的高可靠性提供了保障。双机冗余是系统可靠性设计的常用手段，但如果能很好地利用现有硬件条件来更好的整合整个系统的设计，就会大大节省设计成本。AFS 系统是应用在汽车上的一种智能控制系统，硬件电路设计需要更小的电路板、更好的电磁兼容性，才能更好地在汽车这个高干扰、小空间的场合应用。电路结构如图 2 所示。

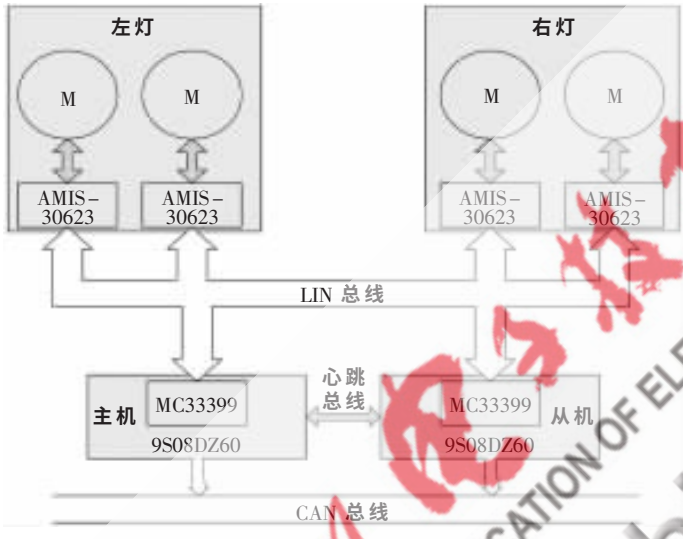

图 2 AFS 控制系统硬件结构图

由于制作工艺不同，芯片的抗电磁干扰能力具有差异性，本系统采用了飞思卡尔 MC9SDZ 系列芯片和安森美的 AMIS-30623 进行设计。主节点芯片 MC9SDZ60 具有独立的 Flash、EEPROM 以及外设接口，并含有一路 CAN 接口，用于与车身 CAN 网络的通信，并通过 TxD1、RxD1 与 MC33399 进行通信，将主机命令转换成 LIN 数据帧向下端 LIN 网络传送。其中 MC33399 作为主节点 LIN 接口与车灯总成部分的 AMIS-30623 进行通信，以达到控制车灯的目的。

两个主从系统可以互不干扰地独立运行相同的任务，主机负责整个系统的控制权，从机作为备机来实现冗余计算，两者之间互为在线监测模块，为软件冗余算法设计提供了硬件基础。

3 软件可靠性设计

软件是一个实时系统的灵魂。软件容错性、软件可靠性等设计是整个系统设计能否成功运行的关键。因此，在可靠硬件的基础上，设计出可靠的实时软件才是整个系统设计的重点。

3.1 主从切换策略

系统上电后，分别对主、从模块初始化。其中主机部分执行主系统，从机部分执行任务系统。从机对主机进行检测，由于车灯控制是一个随机过程，对一种控制策略依赖性过高往往会造成整个系统的性能降低。因而主从系统采用不同的控制算法，从机将得到的运算结果发送给主机，主机根据自己运算的结果和从机的结果进行均值运算，得出最终结果；在通信的过程中进行相互检测，如果有一方发生故障系统仍然能用自己的控制算法控制整个系统，使整个系统继续运行，并进行故障提示，从而提高了系统的鲁棒性。主从切换策略原理如图 3 所示。

3.2 软件子模块划分

主机和从机运行的软件模块大概可以分为 4 个主要模块：主从切换模块、检测模块、控制算法模块、故障处理模块。在主机控制整个系统的前提下，主从机同时从 CAN 网络接收数据，并对其分别用各自的控制算法进行独立运算，主机就会等待从机发来的运算结果。如果等待超时，主机将会认为从机发生故障，并发出故障报警。从机设计检测模块，循环检测主机是否能进入运算结果等待状态。如果主机发生故障，从机将会切换到

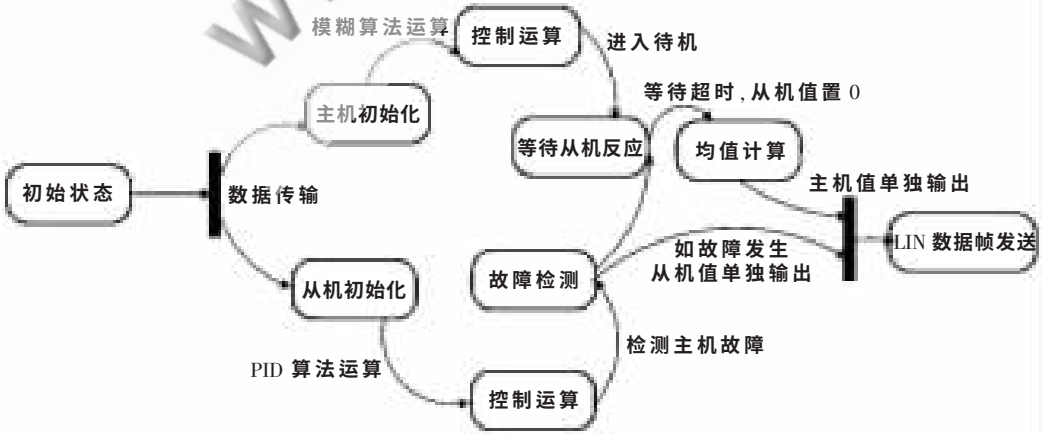

图 3 主从切换状态转移图

单机工作模式并发出主机故障警报。

各功能模块描述如下：

(1)主从切换模块。该模块从检测模块获得调用。主从切换时(即单从机模式)，主机将系统中最新配置信息以及电机反馈过来的实际角位置传递给从机。切换完毕后从机将主动地接收电机的实际角位置反馈，而不再经由主机传送。同时将调用故障处理模块来提醒驾驶者，此时主机进入待维护状态。

主机在等待从机传达运算结果超时的情况下进入从机故障模式(即单主机运行模式)，主机将进行单独运算，并不再把电机实际转角传送给从机，同时将调用故障处理模块来提醒驾驶者，此时从机进入待维护状态。

(2)检测模块。检测模块维护一块动态空间，负责管理接收主机传输的数据。一旦系统上电就开始循环不间断检测心跳总线、主机状态、时钟失步等。一旦检测到故障，即调用切换模块进行工作，同时通过故障处理模块进行处理。

(3)控制算法模块。该模块是整个系统的核心模块，分为主机控制算法模块和从机控制算法模块。由于控制目标的随机性，为了提升整个系统的性能，该模块在主从硬件冗余的基础上实现了控制算法冗余。

(4)故障处理模块。该模块负责系统发生故障后的维护工作，并通过有效手段发出警报，能够使驾驶者及时发现错误，并能够在第一时间维护整个系统，使系统保持主从机同时工作。

4 系统可靠性评估

电子产品的寿命(或失效)要么服从指数分布模型，要么服从 Weibull 分布模型[5]。尽管在很多情况下电子元件指数假设与测试数据相当符合，但韦伯分布每一种情况下都比指数分布的假设更加符合电子元件实际寿命分布[6]，所以被广泛用于电子寿命的预估计。韦伯分布的积累分布函数、可靠度函数、风险函数(失效率)函数分别如式(1)~式(3)(对 $\alpha>0$，$\lambda>0$)[6]所示：

$$F(t)=1-e^{-(\lambda t)^{\alpha}} \tag{1}$$

$$R(t)=e^{-(\lambda t)^{\alpha}} \tag{2}$$

$$z(t)=\alpha\lambda(\lambda t)^{\alpha-1} \tag{3}$$

其中 t 为时间，α 为形状参数，λ 为标量参数。

对整个 AFS 系统硬件、软件层面的分析，在系统正常工作时均值求解模块可以被看作表决器，而当出现故障时又可以看做备用系统，因此本系统是既是备用系统，又含有表决系统的双机双工系统[7]。所以在考虑整个系统的可靠度时，选用两种模型的均值做参考具有合理意义。主从备用系统可靠度[7]为(设主从机失效率均相同)：

$$R_{备}(t)=e^{-(\lambda t)^{\alpha}}\sum_{j=0}^{2-1}\frac{(\lambda t)^{j\alpha}}{j!}=e^{-(\lambda t)^{\alpha}}[1+(\lambda t)^{\alpha}] \tag{4}$$

2 中取 1 表决系统可靠度[7](设主从机失效率相同，表决器失效率为 0，即 $R_d(t)=1$)为：

$$R_{表2\cdot1}(t)=C_2^2(e^{-(\lambda t)^{\alpha}})^2+C_2^1(e^{-(\lambda t)^{\alpha}})(1-e^{-(\lambda t)^{\alpha}})=2e^{-(\lambda t)^{\alpha}}-e^{-2(\lambda t)^{\alpha}} \tag{5}$$

由式(2)、式(4)和式(5)得：

单系统平均无障碍时间：

$$MTBF=t_p=\int_0^{\infty}R(t)dt=\int_0^{\infty}e^{-(\lambda t)^{\alpha}}dt=\frac{1}{\lambda}\Gamma(1+\frac{1}{\alpha}) \tag{6}$$

主从备用平均无障碍时间：

$$MTBF_{备}=t_p=\int_0^{\infty}R_{备}(t)dt=\int_0^{\infty}e^{-(\lambda t)^{\alpha}}[1+(\lambda t)^{\alpha}]dt$$

$$=\frac{1}{\lambda}(1+\frac{1}{\alpha})\Gamma(1+\frac{1}{\alpha}) \tag{7}$$

2 中取 1 表决系统平均无障碍时间：

$$MTBF_{表2\cdot1}=t_p=\int_0^{\infty}R_{表2\cdot1}(t)dt=\int_0^{\infty}[2e^{-(\lambda t)^{\alpha}}-e^{-2(\lambda t)^{\alpha}}]dt$$

$$=\Gamma(1+\frac{1}{\alpha})(\frac{2}{\lambda}-\frac{\sqrt[\alpha]{2}}{2\lambda}) \tag{8}$$

则：

$$R_{总}(t)=\frac{R_{备}(t)+R_{表2\cdot1}(t)}{2}=\frac{e^{-(\lambda t)^{\alpha}}[3+(\lambda t)^{\alpha}]-e^{-2(\lambda t)^{\alpha}}}{2} \tag{9}$$

$$MTBF_{总}=\frac{MTBF_{备}+MTBF_{表2\cdot1}}{2}$$

$$=(\frac{3\alpha+1}{2\alpha}-\frac{\sqrt[\alpha]{2}}{4})\frac{1}{\lambda}\Gamma(1+\frac{1}{\alpha}) \tag{10}$$

其中 $\Gamma(\omega)=\int_0^{\infty}\rho^{\omega-1}\exp(-\rho)d\rho$

由此可以看出，理论上该双机双工系统的可靠度比单系统提高了 $\frac{3+(\lambda t)^{\alpha}-e^{-(\lambda t)^{\alpha}}}{2}$，平均无故障时间比单系统增加了 $(\frac{3\alpha+1}{2\alpha}-\frac{\sqrt[\alpha]{2}}{4})$ 倍。

本文结合 AFS 控制系统工作的特点，对 AFS 控制系统软硬件两方面的可靠性设计进行了充分论证，从理论上分析了系统的可靠性。为汽车 AFS 控制系统设计提供了一个可靠的机电一体化设计方案，对于现有 AFS 系统的升级改造具有一定的指导意义。

参考文献

[1] DOUGLASS B P. Doing hard time: developing real-time systems with UML, objects, frameworks, and patterns[M]. Beijing: China Machine Press, 2005.

[2] 石剑飞，闫怀志. ARM 嵌入式系统可靠性模糊综合评价方法[J]. 科技导报，2009，27(19)：47-51.

[3] 杜军. 提高嵌入式系统可靠性的探讨与实践[J]. 单片机与嵌入式系统应用，2006(4)：15-16，19.

[4] 贾庆忠，刘永善，刘藻珍. 弹载嵌入式系统软件可靠性设计[J]. 微计算机信息(嵌入式与 SOC)，2007，23(26)：2-9.

[5] 胡尧. 关于 Weibull 分布 MTBF 定时实验的置信限[J]. 贵州大学学报(自然科学版)，2006，23(3)：221-223.

[6] SIEWIOREK D P，SWARZ R S. 可靠系统的设计理论与实

践[M].北京:科学出版社,1988.
[7] 汤卫东.硬件冗余技术及可靠性评价[J].广西民族学院学报(自然科学版),2003,9(4):63-67.

(收稿日期:2010-01-21)

作者简介:

张紫瑞,男,1984 年生,在读硕士研究生,主要研究方向:嵌入式软件。

严锐,男,1968 年生,工程师,主要研究方向:计算机辅助设计。

岳继光,男,1961 年生,博导,教授,主要研究方向 :过程控制与计算机控制。