

一种高可靠共轨柴油发动机电控单元

熊建, 顾宏*

(大连理工大学 控制科学与工程学院, 辽宁 大连 116024)

摘要: 柴油发动机电控单元(ECU)是车辆最关键的部件之一,不仅要求系统可靠性高,还要成本低廉.首先对 ECU 失效模式进行了简要分析,然后基于机载计算机硬件容错控制系统理论和软硬件协同优化设计思想,设计并实现了一款具有高可靠性的共轨柴油发动机 ECU.实验结果表明,该电控单元不仅能有效提高系统可靠性,同时还具有成本低、可用性高的优点.

关键词: 电控单元(ECU);硬件容错;双机热备份;仲裁逻辑;共轨发动机

中图分类号: U464.136 **文献标识码:** A **doi:** 10.7511/dllgxb201601009

0 引言

汽车的心脏是发动机,而发动机的电控单元(electronic control unit,简称 ECU)是整个发动机的控制核心.汽车发动机控制器要求系统在具有高可用性、高可靠性的同时,还要求系统的批量成本具有一定优势.因此,汽车发动机 ECU 的设计,既要考虑系统的高可靠性以及汽车发动机控制的运行环境等多种因素,又要考虑系统硬件成本.尤其是中重型的商用车领域的柴油发动机,对终端用户来说,在成本相同的情况下,衡量 ECU 优劣的一个重要标志是其工作可靠性,因为 ECU 的可靠性直接关系到用户的生命财产安全.

柴油发动机 ECU 的基本原理是:首先通过采集发动机的凸轮相位与曲轴转速、冷却水温度、燃油温度、增压压力及中冷后温度等信号来确定发动机的工作状态;然后综合选择恰当的喷油正时与喷油压力,并以最快的方式打开喷油电磁阀,完成喷油过程.

柴油发动机 ECU 控制喷油的过程中,喷油电磁阀的打开过程需要瞬时的高电压和强电流,这部分电路是整个电控单元功率最高、可靠性最低的部分.根据某市公交车指定维修中心的维修记录,在所维修的共轨柴油机公交系统中,80%以上的 ECU 损坏都是在喷油器的驱动电路部分,

尤其以高边 MOSFET 烧坏居多.究其原因,发现这与共轨柴油发动机 ECU 的驱动电路设计及驱动功率大小有关.

进一步分析发现,目前各大公司的做法通常都是把喷油器驱动电路设计为高低边半桥驱动电路.这种驱动电路在喷油器加电的过程中,为了加快响应时间,要求驱动电路首先加上一段远高于电池电压的 BOOST 高电压(该电压值要根据喷油器的机械特性进行优化选择,比如德国 BOSCH 喷油器要求是 48 V,日本 DENSO 早期的喷油器甚至要求 120 V 高压),在这段高电压下,要求电流峰值迅速拉升到一个较大的值(根据喷油器的特性,一般在 18~25 A)以便喷油器快速打开.在这样的高电压、强电流的冲击下,这部分电路经常会出现高边功率开关烧毁断路,或者高边对地短路等严重故障现象,从而使 ECU 完全失效.

航空机载设备由于可靠性的要求极高,通常采用各种基于容错控制理论与硬件容错模型的可靠性设计^[1-4].但是,机载设备对系统成本没有太高的要求,如果完全按照机载设备做冗余控制,就会因过高的产品成本,让客户对产品望而却步.因此,本文在借鉴传统机载设备硬件容错模型的基础上,根据发动机控制系统高边驱动的分时复用原理,将系统硬件仲裁与故障诊断等需要硬件成

本较高的模块利用软件方法来实现,然后分别从软件与硬件两个方面协同优化,使得产品在增加极少硬件成本的情况下,明显提高系统的运行可靠性。

1 硬件容错模型介绍

微电子技术及 VLSI 技术的发展,使得电子元件的体积不断减小,元件产品的成本也不断下降。所以,在对系统可靠性要求较高的机载设备等应用场合中较多采用硬件容错技术。硬件冗余容错技术利用系统资源的冗余和系统结构的实时调整来完成,这种技术主要包括主动、被动、混合等 3 种硬件冗余形式^[5]。

被动硬件冗余(静态硬件冗余)的核心思想是故障掩蔽,即故障情况的变化不会引起冗余结构的变化。二模冗余(twice modular redundancy)和三模冗余(triple modular redundancy)两种结构形式应用最为广泛。如果需要进一步提高系统的可靠性,则还可以增加更多的冗余模块,采用 N ($N>3$) 模冗余(N modular redundancy)结构形式。 N 模冗余结构与三模冗余结构原理相似,只是采用 $N(N>3)$ 个相同的模块。通常 $N=2n+1$ (n 为大于 1 的自然数),目的是易于对系统进行表决,通常的表决原则是少数服从多数。

主动硬件冗余技术通过对系统故障的检测、定位及恢复等几个步骤来完成系统的容错处理,然后对系统结构进行重组,这种技术也被称为动态硬件冗余技术。这种技术通常有 3 种方式,分别是双机比较系统、备用替换系统、成对备用系统。其中,备用替换系统是以一个模块为主模块(master module)在正常工作时产生输出,另外的部分作为备用模块(standby module)。采用各种智能故障检测方法以及智能故障定位技术来确定发生故障的位置与相应的模块。如果主模块发生故障,则系统将进行结构重组,使一个正常工作的备用模块成为主模块。其中备用替换中的备件又可以分为热备份与冷备份两种方式^[4-5]。

冷备份工作模式是指主模块工作时,备份模块不需要加电工作,只有当系统检测并确认系统出现故障,需要备份模块接替工作时才加电并初始化,切换工作模块。

热备份是指系统正常工作情况下,备份模块与主模块同步工作。带热备份的双机比较系统,是

在普通的增强型双机比较的基础上,增加了一个热备份计算机作为备用,而且这种系统中通常带有进行故障定位和检测的自诊断电路。系统开始以双机同时运行,如果检测出系统出现故障,系统将会启动自诊断程序进行故障定位,当定位故障完成后,将故障机从系统中去除并切换到处于正常工作状态的热备份的计算机,系统继续正常运行。

Kim 等便是根据上述增强型双机比较系统模型,去掉比较器、热备份计算机,提出了如图 1 所示的简化的双机热备份系统工作模型,并加以实现^[4]。

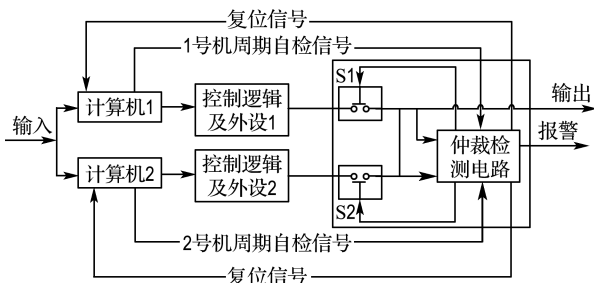


图 1 双机热备份系统工作模型

Fig. 1 Working mode of duplicate hot standby system

如图 1 所示的是基于双机容错的某机载燃油测控系统的工作示意图,系统启动时,1 号机与 2 号机同时工作,但是系统启动时会默认将 1 号机作为主系统输出,而将 2 号机作为热备份机使用(或者相反),且 1 号机和 2 号机各有相对独立的外围设备与控制逻辑,这样做的好处是不会引起系统资源的竞争,同时还能增加整体系统的稳定性。但是,这样会花费更多的硬件设施,系统的硬件成本会急剧增加。另外,如图 1 所示的系统模型中,1 号主机与 2 号备用机之间的切换需要用专门设计的仲裁检测电路来实现,这个仲裁检测电路根据 1 号主机与 2 号备用机周期向它发送的工作状态信息来判断 2 号备用机与 1 号主机的运行状况,并通过控制切换开关 S1、S2 的操作来完成系统切换。这种方案目前在航空机载设备上应用较多,但是汽车发动机的 ECU 与航空设备不同,除了对发动机控制有较强的可靠性要求外,还必须做到成本低廉。而上述方案虽然提高了系统的可靠性和可用性,但其中增加的硬件几乎是单机的两倍,这在汽车工业领域是不可接受的。

传统的发动机工作原理如图 2 所示。喷油器高边一般分为 2 个 BANK,每个 BANK 各自负责

3 个缸的电流调制工作(也有部分 ECU 设计为了节省成本只用一个 BANK 实现电流调制工作). 高边驱动采用分时工作原理,也就是说,考虑到发动机工作时,每个缸不是同时工作的,因此,配合低边驱动的选缸信号,高边驱动不需要用与低边 6 路驱动对应的 6 组高边驱动来完成,理论上讲只需要 1 路即可.

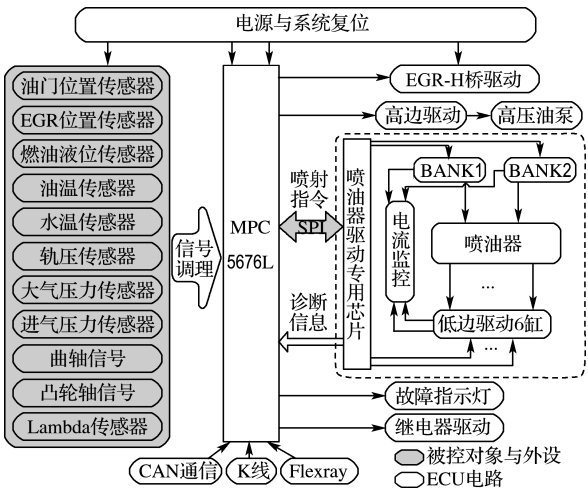


图 2 传统发动机控制单元示意图
Fig. 2 Diagram of traditional ECU of engine

图 2 中虚线部分是传统的 ECU 对电控喷油器的驱动电路. 进一步的示意如图 3 所示. 由图 3 可以看出,在传统的电控喷油器驱动控制方案中大多数采用专用芯片完成对喷油器的驱动.

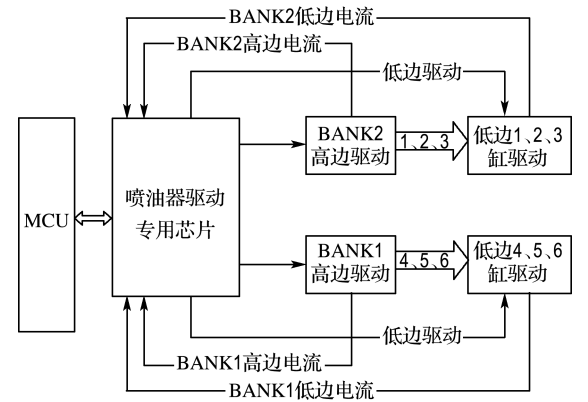


图 3 传统喷油器驱动模式
Fig. 3 Traditional injector driver mode

这样的专用芯片有 Freescale 的 MC33816, 德国 BOSCH 的 CY220 及 CY335 等. 这些专用芯片功能强大,不仅能针对喷油器的特点选择合适的驱动电流波形,而且有较强的故障诊断能力.

但是,用这种专用芯片设计的电路实现的喷油驱动使高边驱动分别各自负责两个 BANK 的工作,一旦其中的一个 BANK 出现了故障,这个 BANK 所对应的几个缸就无法正常工作,整个系统工作就会因此而失效.

因此,为了提高整个 ECU 的工作可靠性及可用性,本文提出一种新的硬件设计方案,只需要在硬件上稍做改动,并通过相应的软件调整,就能避免大量增加冗余硬件,使两个 BANK 不仅可以分时协同驱动喷油器工作,而且还能各自作为独立的冗余单元工作,使得任意一个 BANK 的高边电路出现故障时,系统也能灵活切换到另外一个冗余 BANK 继续工作.

2 硬件设计方案与工作原理

2.1 硬件设计方案

根据上述设计目标,MCU 主控板平台结构如图 2 所示,主控机系统核心处理器采用的是 Freescale 公司的微处理器系列 MPC56xx^[6]. MPC56xx 系列微处理器是 Freescale 公司与 ST 公司基于 Power Architecture 技术的 32 位 Qorivva 微控制器的设计应用. Freescale 公司 Qorivva MCU 系列器件采用功能较强大的高性能 e200z7 系列内核架构,从单核到多核解决方案有广阔的产品线可满足各种汽车应用需求. 同时,该系列 MCU 通过系统架构的一致性、更高的集成能力以及软件和工具的重用性降低了开发成本. 本文采用的是这个系列的一款双核处理器 MPC5676L 微控制器,它是一个专门针对汽车发动机及动力总成控制的符合 ISO26262 安全标准的双核专用芯片. Freescale 公司针对要求严格的汽车电子动力总成等方面安全应用,推出了符合 ASILD 的安全标准,同时在硬件中加入关键安全组件和自测功能,有效降低了软件的复杂程度. 本文采用的汽车级双核微控制器 MPC5676L,采用 32 位数据总线与地址总线. 这种双核单片机与用两个独立的单片机作为冗余备份的方法相比,更具成本低与可靠性高的特点^[7].

本文提出的系统设计目标是在不显著增加硬件成本的基础上,以最简洁的方法实现一个汽车发动机燃油嵌入式容错管理控制系统. 因此,在图 1 所示方案的基础上,提出了一种新型的双机热备份冗余控制模型,如图 4 所示. 在本控制模型

中,针对发动机 ECU 喷油驱动失效问题,巧妙地利用发动机喷油器高边电路分时驱动工作的原理,做了进一步的软件与硬件协同优化与改进,并将其中的双处理器部分与仲裁检测电路部分通过软件来实现,从而节省了大量的硬件资源.图 4 是一个喷油驱动硬件电路优化之后的发动机 ECU 的工作原理示意图.

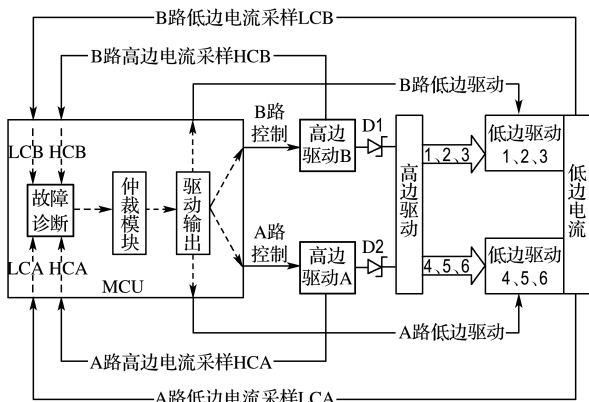


图 4 双机热备份 ECU 工作原理

Fig. 4 The working principle of duplicate hot standby ECU

图 4 所示的软硬件协同优化设计的双机热备份冗余系统模型主要包括硬件驱动电路、电流异常故障诊断管理、仲裁逻辑设计等.系统的主要功能包括高低边驱动电流的采集,系统回路的基本状态自诊断(自测试)逻辑,系统提供低边开关单点故障容错、高边驱动实现双机热切换等.在电路方面的优化主要体现在将传统的驱动方式中 BANK1 与 BANK2 两路通过大电流续流二极管相连,这样改进后的驱动电路实际上并没有直接增加另外两个可以热备份的 BANK1' 和 BANK2',而只是将原有的两个只能负责各自 3 个缸的 BANK 设计成每个 BANK 都可以独立控制所有这 6 个缸,这就相当于将原来的 BANK1 与 BANK2 分成了 A、B 两路独立的驱动,除了可以在软件的协同下像以前一样各自控制 3 个缸,联合一起控制 6 个缸工作以外,还可以让高边驱动 A(BANK1)与高边驱动 B(BANK2) 分别单独驱动 6 个缸工作.

将图 1 中的计算机部分用一个双核的 CPU 代替.同时,考虑到系统的成本以及硬件的复杂度,将图 1 方案中的仲裁检测电路与诊断部分也通过软件模块来实施.通过这样的软硬件协同优

化设计,系统在成本与可靠性之间取得一定的平衡,在原有的系统基础上,几乎没有新的硬件成本的增加,实现了双机冗余系统的可靠性.

2.2 双路容错 ECU 系统工作原理

如图 4 所示,正常工作情况下,系统采用双机工作模式,高边驱动 B 路负责 1、2、3 三个缸的工作,高边驱动 A 路负责 4、5、6 三个缸的工作.系统结构工作原理如图 5 所示.在本系统中,系统可以在 3 种模式下工作:正常工作态、故障态 A 和故障态 B.

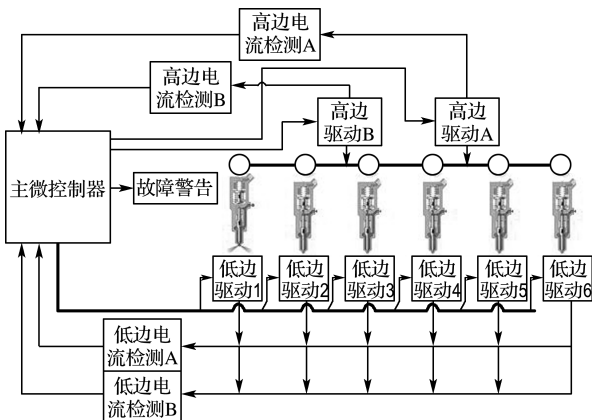


图 5 双机热备份正常工作模式

Fig. 5 Normal working mode of duplicate hot standby

正常工作态下,系统将高边驱动分为 A、B 两个组,轮流控制系统的 6 个缸. A 组高边有一个 $10\text{ m}\Omega$ 高精度的采样电阻,将高边驱动电流转换成电压,经差分放大与调理,然后送入 MPC5676L 的模数转换模块,可以作为电流反馈控制与短路保护依据之一. B 组高边也用同样大小的检测电路.低边驱动电路也是同样分为两个 $10\text{ m}\Omega$ 采样电阻,如前文所述,本文采用与传统做法不同的是,不是将 A、B 两个模块分开,而是将其进行并联(为防止电流倒流,分别在两路增加了功率二极管 D1 和 D2),这样 A、B 两个模块都能单独控制 6 个缸工作,不需要增加额外的硬件就能实现硬件冗余.如图 4 所示,为了表述方便,将系统按 1~6 缸依次排列.

正常状态下的工作时序,按照通常的发动机喷油顺序应该是 1-5-3-6-2-4(6 缸机).其电流驱动顺序与喷油过程为第 1 缸喷油过程:高边驱动 B 打开,负责完成喷油驱动电流波形的调制,同时,低边驱动 1 打开,其他低边驱动关闭,这时电流从 B 到 1 号喷油器通过,1 缸开始喷油.第 5 缸

喷油过程:当高边驱动 A 打开,负责完成另一缸喷油驱动电流波形的调制时,低边驱动 5 打开,其他低边驱动均关闭,这时电流从 A 到 5 号喷油器通过,第 5 缸开始喷油.第 3 缸喷油过程:当准备第 3 缸喷油器打开的时候,由软件系统关闭高边驱动 A,然后用 B 路高边驱动完成喷油驱动波形的调制,低边驱动 3 打开完成选缸,电流从高边驱动 B 经过 3 号喷油器,流经低边驱动 3,完成 3 缸喷油.其他 6、2、4 等各缸工作原理类似,如此,A、B 两模块共同驱动,完成发动机 1-5-3-6-2-4 一个正常驱动的发动机工作循环的喷油过程.

当系统监测到 B 路故障的时候(用高边检测的电流与低边检测的电流作比较,可以很清楚地诊断出系统低边某选缸信号是短路还是开路故障,或是高边驱动出现故障),系统自动关闭 B 路输出,切换为由 A 路系统独立工作.由于原来 B 路与 A 路的输出并联,此时 A 路高边调制信号除了驱动原来的 4、5、6 缸以外,还接替原来 B 路的 1、2、3 缸的高边调制工作,从而依然可以保持驱动 6 个缸正常工作.

同理,当系统检测到 A 路故障的时候,系统切断 A 路高边开关,由 B 路高边开关进行喷油调制信号的处理,此时 B 路开关调制信号除了驱动原来的 1、2、3 缸以外,还要按照正常时序接替原来 A 路的 4、5、6 缸的高边调制工作,从而依然能保持驱动 6 个缸正常工作.

3 软件设计方案与工作原理

3.1 软件设计方案

与硬件可靠性设计中的冗余技术相对应,软件系统的可靠性也有类似的方法.由前面所述,硬件冗余技术主要通过对重要部件及易损部件提供多重备份实现容错,从而提高系统的可靠性^[8].而软件冗余方法主要是利用系统中不同软件模块在功能上的多模块冗余和多模块独立,结合程序设计的解耦来提高整个控制系统的冗余度,从而改善系统的容错性能^[9-12].

本系统设计的高边调制信号端有 A 和 B 两路电流检测,通过采样电阻(本文采用 10 mΩ 高精度电阻),将信号放大滤波等调理之后,送入 MCU 内部的数模转换模块进行模数转换.低边也有两路高精度的电流检测,同样经过信号变换滤波输入数模转换模块进行模数转换.每一次喷

油时刻,MCU 就对当前驱动电流进行采集,然后进行综合判断.

通过对上面 4 组信号进行采样比较,对应的故障状态有高边 A 路与地短路,高边 B 路与地短路(或表现为电流过大,超过限制值);高边 A 路与电源开路,高边 B 路与电源开路(或表现为电流过小,超过限制值,以至于打不开喷油器);低边选缸信号(1~6 缸)与地开路;低边选缸信号(1~6 缸)与电源短路(或电流过小,超过限制值,以至于打不开喷油器).

仲裁与切换是在上述电流异常情况下,综合考虑当前大气压力、进气流量、发动机转速及水温等多种因素之后,确定完成故障处理措施,决定选择何种单机工作模式,保证双机热备份系统的正常工作及出错板极切换,对系统做故障灯指示,对发动机做降功率处理.

3.2 软件系统工作原理

文献[9]对软件可靠性有较清晰的分析.软件系统的可靠性与硬件系统的可靠性不一样,软件系统可靠性只与软件设计质量有关.硬件系统可靠性除了包含硬件设计质量以外,还要包括硬件的物理性质及硬件本身老化衰败对系统可靠性产生的影响.由此可见,软件可靠性与硬件可靠性相比,它对于设计的依赖程度更大一些.另外,在通常情况下,软件可靠性设计准则是由软件开发流程与软件代码的质量来确定的,软件开发流程的目的是用来指导和规范设计人员,给他们提供统一标准的设计依据^[10-11].

本文的软件开发是基于模型的开发方式,利用 Matlab/Simulink 强大的建模与仿真能力,以及 Simulink 下的自动代码生成工具 Embedded coder 将代码生成嵌入式 C 代码,与底层手动编写的基础软件在 Codewarrior 环境下集成编译下载.为了便于模型测试与代码集成,采用手动编写的仲裁逻辑.从可靠性考虑,本文将 A/B 协同工作模块、A 路单机工作模块、B 路单机工作模块等部分分别单独开发,每个模块都可以独立工作,代码以 S-Function 方式加入到 Simulink 模型中,实现了软件驱动的冗余控制,如图 6 所示.

在软件的可靠性设计方面,主要是利用了模块化冗余设计思想.将 A/B 协同工作、A 通道工作、B 通道工作分别写成 3 个软件模块,共享一组数据.同时还有针对发动机保护的余量设计.

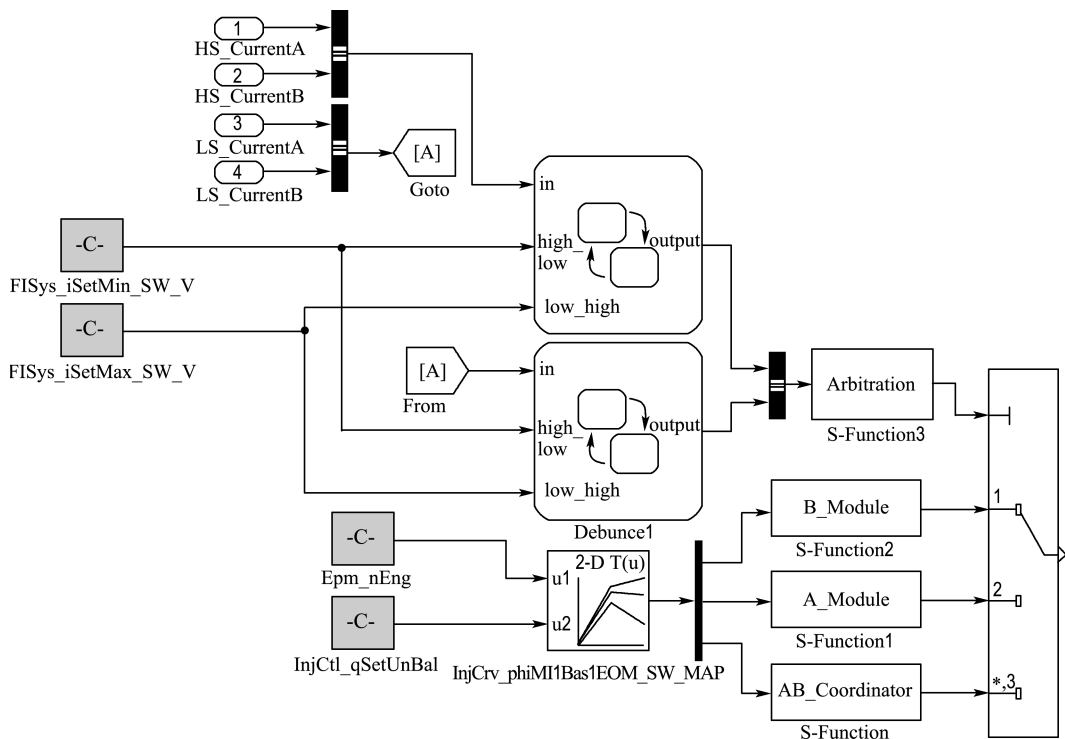


图 6 软件冗余架构

Fig. 6 Architecture of redundant software

由图 6 可见,系统底层分别将 A 通道和 B 通道的高低边电流采样值(变量 HS_CurrentA 表示 A 路高边电流,变量 LS_CurrentA 表示 A 路低边电流,变量 HS_CurrentB 表示 B 路高边电流,变量 LS_CurrentB 表示 B 路低边电流)送入 Debounce 模块进行确认,Debounce 模块的两个极限值用两个标定变量表示,用户可以根据实际情况灵活定义.经 Debounce 模块处理确定后,传递给仲裁模块.如图 4 所示,针对 3 种工作模式分别设计了 3 个模块,系统正常工作时,也就是系统默认的为 A/B 协同工作,并将工作状态参数 3 传递给变量 InjCtl_stOfDriver (驱动电路状态变量),表明系统处于正常工作状态.当仲裁模块判断 A 通道出故障时,仲裁输出值为 1,这时系统切换到 B 模块工作,同时工作状态参数 1 传递给变量 InjCtl_stOfDriver,表明系统处于单机 B 工作状态,需要通过故障灯指示维修,以及功率限制模块限制发动机的功率输出;同理,当仲裁模块判断 B 通道出故障时,仲裁输出值为 2,这时系统切换到 A 模块工作,同时工作状态参数 2 传递给变量 InjCtl_stOfDriver,表明系统处于单机 A 工作状态,需要通过故障灯指示维修,以及功率限制模块限制发动机的功率输出.

3.3 系统可靠性分析

系统可靠性是指被分析对象所具有的在一段时间内,在给定条件下,完成指定功能的特征.也即被定义为在特定时间周期内实现预期功能的能力.为了便于衡量和研究系统可靠性,首先定义与可靠性函数相关的几个概念^[12-13].

定义 1 无故障时间 (time to failure),研究大量单元数目 ($i=1,2,3,\dots,N$),观测单元 i 能正常工作的期间内的时间 T_i ,称为观测单元 i 的无故障时间.

定义 2 相关故障频率 (relative cumulative failure frequency),同样条件下的多个相似观测单元的相关故障频率 $\hat{F}(t)=n(t)/N_0$.这里的 N_0 是指在 $t=0$ 的起始时刻的观测单元数, $n(t)$ 表示系统正常运行 t 时间以后,观测单元出现故障的数量. $\hat{F}(t)$ 也称为经验故障函数^[12].

定义 3 经验可靠性函数 $\hat{R}(t)=[N_0-n(t)]/N_0=1-\hat{F}(t)$.

依据大数定理,当 N_0 取无穷大时,故障发生的频率就可以看成故障概率 $F(t)$.相对应地,故障发生的概率的补集 $R(t)=1-F(t)$ 就是经验可靠性函数.因此, $R(t)$ 就是观测单元在 $0\sim t$ 时间

间隔期间处于能够正常工作的概率^[12].

在中重型的发动机控制系统正式装车前,一般要求系统具有 2 000 h 的可靠性实验.对 ECU 器件的无故障时间要求是 2 000 h,因此,其可靠性 $R(t)=1-F(t)=1-0.000\ 5=99.95\%$.

利用本文提出的方案,系统的可靠性 $R(t)=1-0.000\ 25=99.975\%$,由此可见,本文所提出的系统采用双机冗余备份的方案,系统只多增加了一路低边采样电阻,与单路高边调制 ECU 方案相比,只部分增加了一路驱动(注:当前很多中重型 ECU 高边驱动被设计成两路,分时控制两个 BANK,与这种方案相比,本系统高边部分没有增加硬件成本,只需要高边驱动 MOSFET 适当提高功率参数即可).相对于整个 ECU 而言,硬件成本只增加不到 2%,系统的可靠性明显提高,从而显著提高了系统的可用性.

4 实 验

根据本文所提出的设计思想,设计了一款高可靠性 ECU,如图 7 所示.接插件采用 Tyco 公司生产的型号为 284617 的端子,该接口与德国 BOSCH 公司的 EDC17C35 针脚一致.在硬件设计时,将电源、传感器、执行器的针脚定义也尽量与该型号 ECU 兼容,以便可以直接替换 ECU.

在实验中分两个方面进行验证.一方面,在实际油量测试台与发动机台架测试.首先在装有 BOSCH 原装喷油器的冷拖实验台上进行了 2 000 h 的冷拖实验.冷拖实验完成之后,将同一 ECU 安装在 1 台装有 BOSCH 共轨燃油系统的某重型发动机上进行 2 000 h 的热机可靠性测试.实验结果表明,该 ECU 完全满足设计要求.

另一方面,将本文所设计的 ECU 在自行研制的可靠性模拟实验台上进行半物理仿真测试.实验中,分别人为制造出 A 路高边驱动和 B 路高边驱动短路及开路系统故障,结果表明,在这两路高边分别出现故障态时,系统检测到故障并能顺利切换到备用通道工作,达到了预期的设计目标.同时,为了更进一步对小批 ECU 进行可靠性测试,在可靠性模拟实验台上设计了多组发动机信号模拟器,可以同时模拟出多个发动机曲轴(60—2 齿)磁电转速信号和凸轮(6+1 齿)霍尔相位信号,按照某重型发动机(配 BOSCH 的原装燃油系统和控制系统)的极限工作工况,设置每工作循环

3 次喷射(预喷+主喷+后喷),驱动负载采用某国产电控喷油器实物进行模拟喷油测试.对 10 套新型 ECU 进行全速全负荷运行 4 000 h 的模拟实验,结果表明系统的稳定性较传统设计的电控单元有明显提高.验证结果进一步表明,本文设计的 ECU 可靠性完全达到了预期的容错功能.

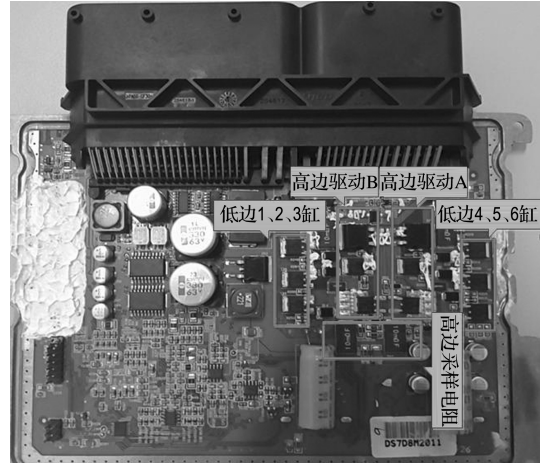


图 7 高可靠性 ECU 电路板

Fig. 7 The real PCB of highly reliable ECU

5 结 语

初步实验结果表明,本文所设计的电控单元具有系统可靠性高、通用性强、成本低等优点,有很强的实用性和市场推广价值.目前,该系统已在基于汽车电子嵌入式安全实时操作系统 OSEK Turbo 的支持下,开发完成上层应用软件的主体控制软件,正在进行整车标定实验,随后将进一步进行批量整车的验证工作.

参考文献:

- [1] 周东华. 容错控制理论及其应用[J]. 自动化学报, 2000, 26(6):788-797.
ZHOU Dong-hua. Theory and applications of fault tolerant control [J]. *Acta Automatica Sinica*, 2000, 26(6):788-797. (in Chinese)
- [2] Wensley J H, Lamport L, Goldberg J, et al. SIFT: Design and analysis of a fault-tolerant computer for aircraft control [J]. *Proceedings of the IEEE*, 1978, 66(10):1240-1255.
- [3] Hopkins Jr A L, Smith III T B, Lala J H. FTMP - A highly reliable fault-tolerant multiprocessor for aircraft [J]. *Proceedings of the IEEE*, 1978, 66(10):1221.

- [4] Kim K H. Issues insufficiently resolved in century 20 in the fault-tolerant distributed computing field [J]. **Proceedings of the IEEE Symposium on Reliability Distributed Systems**, 2000:106-115.
- [5] 熊建,熊光泽. 一种高可靠测控计算机的设计与实现[J]. **计算机测量与控制**, 2005(7):671-673, 695.
XIONG Jian, XIONG Guang-ze. Design and realization of a highly reliable measuring and control computer [J]. **Computer Measurement & Control**, 2005(7):671-673, 695. (in Chinese)
- [6] Freescale Semiconductor, Inc.. **MPC5676L User's Manual and Datasheet** [M]. Austin: Freescale Semiconductor, Inc., 2012.
- [7] 衡军山,甄成刚. 基于软件的双CPU冗余控制研究[J]. **微计算机信息**, 2005, 21(7):59-61.
HENG Jun-shan, ZHEN Cheng-gang. Research on CPU redundancy control based on software [J]. **Microcomputer Information**, 2005, 21(7):59-61. (in Chinese)
- [8] 陈宇. 高可靠容错实时系统的支撑技术研究[D]. 成都:电子科技大学, 2002.
CHEN Yu. Research on supporting techniques for high-reliable fault tolerant real time systems [D]. Chengdu: University of Electronic Science and Technology of China, 2002. (in Chinese)
- [9] 刘遒. 软件可靠性设计技术应用研究[D]. 长春:中国科学院长春光学精密机械与物理研究所, 2013.
- LIU Luo. Study on the application of software reliability design technology [D]. Changchun: Changchun Institute of Optics, Fine Mechanics and Physics, Chinese Academy of Sciences, 2013. (in Chinese)
- [10] 张治生,陈怀民,吴成富,等. 小型无人机飞控系统软件可靠性设计与建模研究[J]. **计算机测量与控制**, 2011, 19(6):1489-1492.
ZHANG Zhi-sheng, CHEN Huai-min, WU Cheng-fu, *et al.* Research of software reliability designing and modeling of flight control system of SUAV [J]. **Computer Measurement & Control**, 2011, 19(6):1489-1492. (in Chinese)
- [11] 陆志肖,聂永显,谢剑斌,等. 软件可靠性设计在机电管理系统软件中的应用[J]. **直升机技术**, 2010(3):53-58.
LU Zhi-xiao, NIE Yong-yu, XIE Jian-bin, *et al.* The application of the soft reliability design on the UMS's soft [J]. **Helicopter Technique**, 2010(3):53-58. (in Chinese)
- [12] 绍弗勒 J. 汽车软件工程——原理、过程、方法、工具[M]. 张聚,等译. 北京:电子工业出版社, 2008.
Schauffele J. **Automotive Software Engineering Principles, Processes, Methods, and Tools** [M]. ZHANG Ju, *et al.* trans. Beijing:Publishing House of Electronics Industry, 2008. (in Chinese)
- [13] Birolini A. **Reliability Engineering — Theory and Practice** [M]. 3rd ed. New York:Springer, 1999.

A highly reliable ECU of common rail diesel engine

XIONG Jian, GU Hong*

(School of Control Science and Engineering, Dalian University of Technology, Dalian 116024, China)

Abstract: The electronic control unit (ECU) of diesel engine is a key module of the vehicle. It requires not only the high reliability but also the low cost. Firstly, the failure mode of ECU is analyzed briefly. Then, based on the theory of airborne computer fault-tolerant control system and co-design method of software and hardware, a kind of highly reliable ECU of common rail diesel engine is designed and implemented. The experimental results show that this ECU can not only improve the reliability of system effectively, but also has the advantages of low cost and high availability.

Key words: electronic control unit(ECU); hardware fault tolerance; duplicate hot standby; arbitration logic; common rail engine