2015 年大功率柴油机分会智能化与控制学组技术交流会专栏

柴油机控制系统冗余热备份设计技术研究

李文辉，刘　龙

(哈尔滨工程大学动力与能源工程学院,黑龙江 哈尔滨 150001)

摘　要：控制系统的可靠性对于保证电控柴油机的正常工作具有重要意义。结合 396 系列柴油机综合电控系统的研制,分析了包括冗余技术在内的提高柴油机电控系统可靠性的技术手段,重点分析了冗余热备份系统需要解决的关键技术与技术途径,并对该系统存在的不足与改进措施进行了分析。

关键词：柴油机;控制系统;热冗余

中图分类号:TK424.3　　**文献标识码**:A　　**文章编号**:1001 -4357(2016)01 -0010 -04

Research on Design of Hot Redundancy Backup of Diesel Engine's Control System

Li Wenhui, Liu Long

(College of Power and Energy Engineering, Harbin Engineering University, Heilongjiang Harbin 150001)

Abstract: The reliability of control system plays an important role in ensuring the normal operation of electronic control diesel engine. Based on the development of 396 series diesel engine integrated electronic control system, technical means including redundancy technology which can improve the reliability of diesel engine's electronic control system are studied. The key technologies and technical solutions for hot redundancy backup system are analyzed in detail, and the deficiency and improvement methods are also studied.

Key words: diesel engine; control system; hot redundancy

0　引　言

目前高性能柴油机普遍采用电子控制技术，控制系统的可靠性对保证柴油机正常运行极为重要，特别是在一些关键应用领域，更是要求在控制系统出现故障情况下仍可以维持柴油机的运行。常用的提高控制系统可靠性的措施主要有：从工艺上提高构成系统的元器件的可靠性，对元器件进行严格的筛选；优化设计；规范装配与测试等工艺过程；采取屏蔽减少外部干扰等[1-3]。这些常规技术已被广泛应用，并在提高系统可靠性方面起到了重要作用。但总的来说，这些常规技术目的还是降低控制系统出现故障的概率，属于“避错”技术。但仅仅“避错”还满足不了那些对可靠性要求更高的领域，需要采用即使在系统出现故障时仍可以保证控制系统主要或全部功能不丧失的设计技术，即容错技术。所谓容错，是指处于工作状态的系统中一个或多个关键部分发生故障或出错时，能够实现自动检测与诊断，并能采取相应措施保证系统维持其规定功能或保持其功能在可接受的范围内[2]。

实现容错设计常用的技术措施是冗余设计，通常有两种冗余方式：热冗余和冷冗余。所谓热冗余，是指系统具有相同的两个单元同时工作，一个为正常工作状态，具有完整的数据处理与控制功能，另一个工作在备用状态，可以处理部分数据，但不输出控制信号。当正常工作用的控制单元出现

收稿日期：2015-06-25

作者简介：李文辉(1971 -)，男，教授，主要研究方向为柴油机智能与综合电子控制系统，E-mail：li-wenhui@ hotmail. com。

故障时，系统应能够自动切换到备用单元，保证被控设备工作的连续性。至于冷冗余系统，只有一套系统处于工作状态，当工作系统出现故障时，需要停机并人工更换备用系统。因此，冷冗余不能保证故障时被控设备运行的连续性，严格来说并不算是冗余，仅仅是一种备件形式[4]。

要实现在柴油机电控系统出现故障的情况下仍可以维持柴油机不间断的运行，必须采用热冗余技术。由于控制对象——柴油机具有多输入、多输出特点，在设计热冗余控制系统时需要考虑：哪些输入、输出接口需要冗余，如何保证热冗余系统故障诊断与控制切换的可靠，以及如何避免故障系统对工作系统的干扰等问题。本文结合 396 系列柴油机综合控制系统（以下简称 ECS 系统）研制的经验，就这些问题进行探讨。

1　396 柴油机综合电控系统冗余设计

根据 396 系列柴油机安装运行状态监测传感器与控制执行器件对柴油机运行的影响，其输入信号、输出信号可分为普通类型和安全类型。对于普通信号，如进气压力、排气温度等，这些参数可以参与对柴油机的优化调节，但这些参数的缺失并不会对柴油机的运行造成太大影响。而另外一些参数，如润滑油压力、柴油机转速等，在柴油机运行中如果这些参数传感器或输入电路发生故障，且不能及时发现、处理，有可能会对柴油机造成不可逆转的损害；又如当柴油机转速测试不正常时，将导致柴油机不能运行——停机或飞车；此外，操作输入或控制单元微控制器故障也会导致对柴油机的控制、调节功能丧失。对这些涉及柴油机运行安全的输入信号与控制信号须要采用冗余设计。

1.1　控制系统输入输出结构

根据对容错功能要求的不同，控制系统输入输出结构有 1oo1、1oo2、2oo2、1oo1D、2oo2D、2oo3 等几种类型[5]，其中常用的为 1oo1 和 2oo2 类型。1oo1 系统（如图 1）的输入输出由单通道实现，因而不具有容错功能，也不具有失效模式保护功能，但其实现方式简单。2oo2 系统（如图 2）采用冗余结构，对于一个参数采用两路输入/输出回路处理，这种结构具有一定的容错功能。

考虑到 396 柴油机现有传感器与执行机构的安装接口，ECS 系统在设计上综合了 1oo1 和 2oo2 两种结构，如图 3 所示。对于普通输入信号，例如进气温度、进气压力、海水温度等，每个参数只安装一支传感器，该传感器只接入主 ECS 输入接口，由主 ECS 进行处理。对于润滑油压力、冷却水温度、油泵齿条位移等安全类输入则采用两支传感器，分别接入主、备 ECS 输入接口。

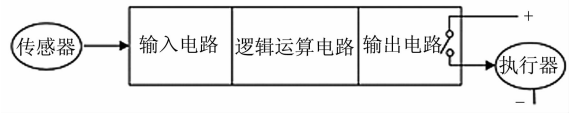

图 1　1oo1 结构

图 2　2oo2 结构

另外，所有输出控制接口由主、备 ECS 进行并联控制。正常情况下，由主 ECS 对柴油机进行调节、控制；备 ECS 工作在备用状态，仅在主 ECS 的齿条位移、柴油机转速等关键信号失效，或主 ECS 微控制器故障时，备 ECS 才进入对柴油机进行控制与调节的工作状态。

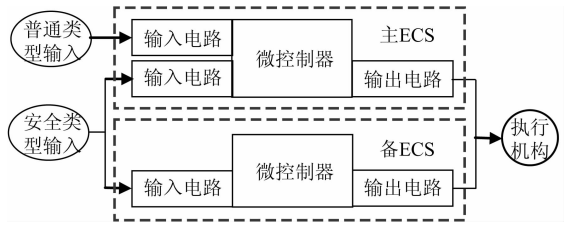

图 3　ECS 系统输入输出结构

1.2　主、备 ECS 冗余热备份原理

首先解释一下本文中主 ECS、备 ECS、工作 ECS 和备用 ECS 的含义。冗余热备份 ECS 系统由两个 ECS 单元组成，一个称为主 ECS，具有完整的柴油机测试与控制接口，正常情况下由主 ECS 对柴油机实施控制；另一个称为备 ECS，具有部分柴油机测试和全部控制接口，正常情况下作为备用，仅在主 ECS 故障时才对柴油机进行调节控制。在柴油机运行时，主、备 ECS 实际上只有一个对柴油机具有控制权，其中具有控制权的称为工作 ECS，另一个不具有控制权，但可以实时监测工作 ECS 的工作状态，一旦工作 ECS 出现故障可以迅速接管对柴油机控制权，称为备用 ECS。因此，主 ECS 和备 ECS 是冗余热备份 ECS 系统的组成，而工作 ECS 和备用 ECS 是描述 ECS 的工作状态。

如前所述，由于柴油机输入、输出接口很多，特别是很多终端执行机构同时受控于主、备 ECS，

对于主、备 ECS 的设计，除了考虑一般的冗余热备份系统主、备系统故障侦测与切换外，还需要针对柴油机实时控制的稳定性，考虑系统切换的稳定性与可靠性、故障系统输出的隔离屏蔽等问题，避免失效系统可能出现的错误输出对正常系统控制功能的影响。针对柴油机控制系统的特殊要求，本文所研制的 ECS 系统冗余热备份实现原理如图 4 所示。

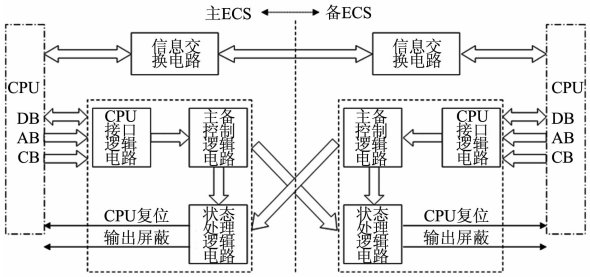

图 4　冗余热备份系统原理

该冗余热备份实现方式由信息交换电路、CPU 接口电路、主备控制逻辑电路和状态处理逻辑电路组成[6,7]。

其中，信息交换电路用于主、备 ECS 系统传递心跳数据，交换测试和控制数据。当系统工作时，一方面主、备 ECS 通过信息交换电路相互发送和接收心跳报文，以确定对方微控制器是否运行，一旦备用 ECS 系统检测到工作 ECS 系统心跳报文静止，将立即切换到工作状态；同时通过 CPU 接口逻辑电路和主备控制逻辑电路输出切换控制信号，实现对故障 ECS 输出信号的屏蔽处理，输出自己控制信号。另一方面，为保证控制权切换后控制输出保持连续稳定，工作的 ECS 周期性地将各种柴油机运行控制参数通过信息交换电路发送给备用 ECS，在发生控制权切换后，备用 ECS 可以在切换后以事先接收到的数据作为控制初始参数，实现平稳过渡。

信息交换电路的另一个作用是可以实现主、备 ECS 共享冗余传感器的测试数据。例如，当主 ECS 润滑油压力传感器发生故障而备 ECS 润滑油压力测试正常时，备 ECS 会将润滑油压力测试数据通过信息交换电路共享给主 ECS，维持主 ECS 监测参数的完整性。

本系统的信息交换电路采用双口 RAM 实现。相对于采用通讯总线的信息交换方式，双口 RAM 具有通讯速度快、软件设计简单等优点。本系统的双口 RAM 实际使用时被分为三个区域：主 ECS 写-备 ECS 读（MEBR）区域、备 ECS 写-主 ECS 读（MRBW）区域和工作 ECS 写-备用 ECS 读（WWIR）区域。主 ECS 工作时周期性地向 MEBR 区域更新心跳报文数据和测试参数等信息，备 ECS 通过读取 MEBR 区域的心跳报文数据判断主 ECS 是否运行，同时读取主 ECS 测试的柴油机运行数据。类似地，MRBW 区域用于备 ECS 向主 ECS 传输相关数据。WWIR 区域由于主 ECS 和备 ECS 交换柴油机运行时的控制数据，由取得控制权的 ECS 负责更新 WWIR 区域数据，处于备用状态的 ECS 通过读取 WWIR 区域数据保持控制状态同步。

CPU 接口逻辑电路、主备控制逻辑电路和状态处理逻辑电路组成冗余热备份 ECS 主备切换控制接口。这些接口电路均通过组合逻辑实现，避免单一逻辑信号在受到干扰时可能产生的扰动和处理器故障时逻辑控制的失效。CPU 接口逻辑电路的输入端作为一个数据端口和微控制器的数据总线连接，由微控制器通过对该端口写入特定的组合数字，主备控制逻辑电路根据有效的输入组合，产生供给本机的状态处理逻辑电路信号和供给另外一个 ECS 主备控制逻辑电路的组合逻辑。同样，状态处理逻辑电路输入包括连接本机控制逻辑电路的内部输入，和连接另外 ECS 控制逻辑输出的外部输入。外部输入同样为组合逻辑，例如用 10101010 表示本机取得控制权，禁止对方控制输出，复位对方为控制器；用 10100101 表示取消对对方微控制器的复位但保持输出屏蔽；01010101 组合逻辑用于在对方 ECS 恢复运行后可以通过本机控制屏蔽本机输出时取消对对方输出的屏蔽控制。而其他未定义的组合均认为是无效输入，避免个别信号受到干扰引起冗余切换误动作。

冗余控制接口的状态处理逻辑电路的输出为“CPU 复位”信号和“输出屏蔽”信号。在某 ECS 因微控制器故障而不能运行时，取得控制权的 ECS 会通过主备控制逻辑电路产生复位信号，用于对故障 ECS 进行复位操作，尝试恢复故障 ECS 的微控制器运行。“输出屏蔽”信号在本机微控制器运行正常时，由本机微控制器通过组合逻辑产生输出，在本机取得控制权作为工作 ECS 运行时，“输出屏蔽”信号无效，本机微控制器可以通过驱动电路对柴油机终端执行器件输出控制信号；在本机为备用状态时，“输出屏蔽”信号屏蔽本机的控制输出接口，避免本机控制输出干扰工作 ECS 对柴油机的控制。在本机微控制器故障时，“输出屏蔽”由外部输入组合逻辑产生，避免在微控制器失效期间控制电路的不确定状态影响工作 ECS 对柴油机的控制。

冗余热备份系统切换接口电路的可靠度与组合

逻辑的位数有关，组合逻辑位数越多，误动作的概率就越小，但增加组合逻辑的位数也会增加接口电路的复杂性，实际设计时需要根据从器件接口、连接方式等因素均衡考虑。在本系统中微控制器与 CPU 接口逻辑采用 16 位宽度，而主、备 ECS 之间的控制逻辑与状态逻辑接口采用 8 位宽度。

1.3　主备 ECS 状态逻辑与切换

冗余热备份 ECS 系统主、备 ECS 的工作状态均包括复位状态、初始化状态、工作状态、备用（待机）状态和故障状态，如图 5 所示。系统上电后，首先进入复位状态，然后进行自检和参数初始化，初始化完成后默认主 ECS 首先进入工作状态，然后备 ECS 进入备用状态。

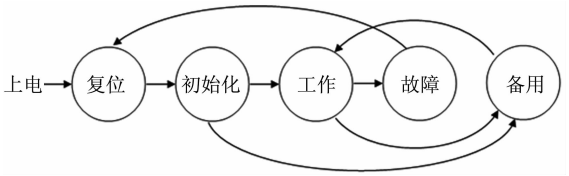

图 5　主、备 ECS 状态逻辑图

一般情况下，主 ECS 始终处于工作状态，对柴油机实施监控。从主 ECS 工作切换到备 ECS 工作一般有两种情况：一种是主 ECS 故障，包括关键输入、输出故障或微控制器故障。在关键输入、输出故障情况下，主 ECS 通过信息交换主动通知备 ECS 接管控制权，主 ECS 进入故障状态。如果是主 ECS 微控制器故障，本身已不具备与备 ECS 进行信息交换功能，则由备 ECS 根据主 ECS 心跳报文异常主动获取控制权，同时输出组合逻辑屏蔽主 ECS 输出、尝试复位主 ECS 微控制器，主 ECS 进入故障、复位状态。在这种情况下，当主 ECS 复位恢复正常后，备 ECS 会主动交出控制权，由主 ECS 完成对柴油机的调节控制。第二种切换情况是由操作人员通过外部按键输入“主备切换”控制指令，在收到该指令后，如备用 ECS 正常，则工作 ECS 通过信息交换通知备用 ECS 接管控制权，如备用 ECS 故障，则切换指令被忽略。

2　主备 ECS 切换试验

试验对象为某型 396 柴油机发电机组，柴油机额定转速为 1 800（r · min^{-1}），稳态运行转速波动率 <0.5%（±9（r · min^{-1}）），瞬时转速波动率 <0.5%（±90（r · min^{-1}）），转速恢复到额定转速 ±0.5% 时间小于 3 s。表 1 为配备冗余热备份 ECS 系统的 396 柴油机进行主-备切换试验的结果。

图 6 为机组 1 ~ 机组 4 切换过程中记录的柴油机转速变化曲线。每次试验包括从主 ECS 切换到备 ECS 和从备 ECS 切换回主 ECS 两次切换，因此有两次转速波动。一般情况下转速波动在 ±15（r · min^{-1}）以内，也有个别机组偶尔发生切换时转速波动约 2.5% 的情况。由试验结果可以看出：主、备 ECS 切换后柴油机可以保持连续运行，切换过程中柴油机转速有小幅波动。

表 1　主备切换试验

序号	转速/（r · min^{-1}）		最大转速波动率	恢复时间/s
	最低转速	最高转速		
机组 1	1 785	1 814	0.83%	0.3
机组 2	1 785	1 815	0.83%	0.4
机组 3	1 787	1 812	0.72%	0.4
机组 4	1 792	1 807	0.44%	0
机组 5	1 785	1 812	0.83%	0.6
机组 6	1 785	1 814	0.83%	0.5
机组 7	1 791	1 845	2.50%	2.1
机组 8	1 791	1 809	0.50%	0

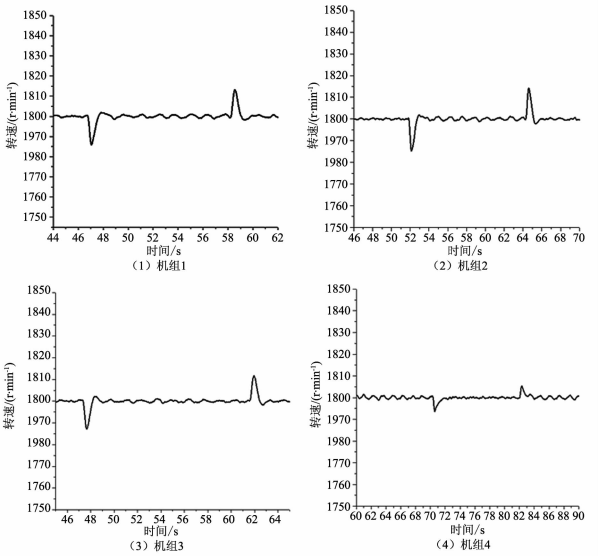

图 6　机组 1 ~ 4 主备切换时转速变化

3　存在的不足与改进措施

由试验结果可以看出，冗余热备份 ECS 在进行主、备切换时，虽然可以保持柴油机连续稳定运行，但在切换瞬间还是会产生转速波动，波动幅度虽然没有超过瞬态转速波动范围限值，但多数情况下均超过稳态转速波动范围限值。究其原因，主要有以下几面：

（1）主、备 ECS 齿条位移传感器零点和信号调理回路不一致。由于位移传感器零点不一致，导致在同一柴油机运行状态下，主、备 ECS 对齿条的测试结果存在偏差，切换后就会造成转速控制环

节内齿条位移参数出现跳跃，造成柴油机油量调节出现变化，引起柴油机转速波动。同样，主、备 ECS 齿条位移传感器敏感度与信号调理回路参数不一致也会导致类似的后果。

（2）主、备 ECS 执行器驱动回路性能参数一致性不高。执行器驱动回路由执行器驱动线圈、驱动 MOS 管等组成，当这些部分的电气或电磁性能存在偏差时，甚至线路阻抗不一致时，在系统切换同样控制输出后也会导致驱动电流变化，继而导致控制油量的执行器齿杆位置发生变化，引起柴油机转速波动。

针对零点误差，可以通过提高位移传感器的装配精度进行改善；对于位移传感器敏感度与信号调节回路不一致性，则可以通过元器件筛选、匹配进行提高，也可以通过精确标定对系统误差进行修正。对于执行器驱动回路一致性，通过改进执行器加工工艺，改善执行器与电缆装备，可在一定程度上有所提高，但要完全消除这种不一致性存在一定难度。

4 结 论

本文所提出的柴油机控制系统冗余热备份实现方法，可以有效屏蔽故障系统对工作系统干扰；采用组合逻辑可提高切换控制的稳定性与可靠性，而且通过逻辑电路实现状态控制与状态处理，可有效避免 ECS 系统微控制器故障对系统切换功能的影响。实际应用也表明：该冗余系统切换控制方法合理可行。

参考文献

[1] 叶昕. 飞行控制计算机双机热备份技术研究 [D]. 南京：南京航空航天大学，2004.

[2] 唐仁杰. 列车控制车载子系统双机容错模拟研究 [D]. 成都：西南交通大学，2007.

[3] 宋百玲，宋恩哲，李金华，等. 柴油机双机热备份电子调速系统设计研究 [J]. 内燃机工程，2009（2）：20-24.

[4] 陈子平. 浅谈控制系统冗余控制的实现 [J]. 自动化仪表，2005，26（9）：4-6.

[5] Goble，M William. Control system safety evaluation & reliability [M]. ISA c1998 2nd ed.

[6] 李文辉，石勇，费红姿. 发动机冗余电控系统切换控制方法 [P]. 中国：CN101430550，2009-05-13.

[7] 李文辉，石勇，费红姿. 发动机冗余电控系统切换电路及控制方法 [P]. 中国：CN100492223，2007-09-05.

（上接第 4 页）

5 结论

根据目标发动机凸轮和曲轴信号的特点，研究了超高压共轨系统位置同步的方案，得到了时序控制的方法，利用 eTPU 完成了设计与实现。软件测试表明：基于 eTPU 的超高压共轨系统位置同步快速可靠，增压和喷油时序控制准确，达到了预期目的。

参考文献

[1] 汪洋，谢辉，苏万华，等. 共轨式电控喷射系统控制参数对柴油机燃烧过程及排放的影响 [J]. 燃烧科学与技术，2002（3）：258-261.

[2] Leonhard R，Warga J. 2000 bar diesel common rail by bosch for passenger cars [J]. MTZ，2008，69（10）：26-31.

[3] Meek G，Williams R，Thornton D，et al. Ultra high pressure distributed pump common rail system [C]. SAE 2014-01-1440，2014.

[4] Matsumoto S，Date K，Taguchi T，et al. The new DENSO common rail diesel solenoid injector [J]. MTZ，2013，74（2）：44-48.

[5] Leonhard R，Parche M，Alvarez-Avila C，et al. Pressure-amplified common rail system for commercial vehicles [J]. MTZ，2009，70（5）：10-15.

[6] 陈海龙，欧阳光耀，张静秋. 增压式高压共轨系统新型电控增压泵研究 [J]. 内燃机工程，2011，32（5）：44-48.
Chen H L，Ouyang G Y，Zhang J Q. Research on new electron-controlled booster applied to augment high pressure common-rail system [J]. Chinese Internal Combusion Enginerring，2011，32（5）：44-48.