·自动化技术·

三重化冗余多机系统心跳检测机制研究

邹见效，张正迁，徐红兵

(电子科技大学自动化工程学院 成都 611731)

【摘要】以汽轮机三重化冗余危急跳闸系统为对象，研究了用于多主多从结构高可靠系统的心跳故障检测机制。采用PUSH模式结合PULL模式的心跳检测方法，减小了系统的误判率；针对三重化冗余系统的特点，结合不同控制器节点在系统中起的作用，将系统通信模式设定为多主多从结构。采用分级心跳检测机制和把心跳信息融入系统周期性传输数据中的方法，减少了故障检测的通信开销。仿真及实际应用结果证明了该方法的有效性和可靠性。

关 键 词 心跳检测； 主从结构； 多机系统； 三重化冗余

中图分类号 TN713 文献标识码 A doi:10.3969/j.issn.1001-0548.2010.03.012

Study on the Heartbeat Mechanism for Triple Modular Redundant Multi-Machine System

ZOU Jian-xiao, ZHANG Zheng-qian, and XU Hong-bing

(School of Automation Engineering, University of Electronic Science and Technology of China Chengdu 611731)

Abstract A heartbeat monitor mechanism which is designed especially for the multi-machine system with high reliablity is introduced. With the turbine triple modular redundant emergency trip system as research object, the experimental system is designed to be multi-master and multi-slave structure. The heartbeat monitor model combining PUSH and PULL can decrease the misdiagnosis rate greatly. Simulation results and field commissioning prove the effectiveness and reliability of this mechanism.

Key words heartbeat; master-slave structure; multi-machine system; triple modular redundancy

汽轮机危急跳闸系统(ETS)[1-2]用于监控机组安全，在某些参数超过安全限值时，发送出紧急停车信号，避免危险扩散造成巨大损失，对于生产装置的安全、稳定、高效运行具有重要意义。三重化冗余(TMR)容错控制技术[3-4]是近年来发展起来的一种容错设计技术，在航空航天、军事、铁路、石油、化工、电力等高可靠性要求的行业得到了广泛的应用。三重化冗余ETS系统将所有模块进行三重化配置，以达到提高系统的可靠性和安全性的目的，可极大提高系统的可靠性。在三冗余ETS系统中对各模块的失效检测是一个非常重要的指标，高效、实时、可靠的失效检测方法对于保障三重化冗余危急跳闸系统的可靠性[5]具有重要意义。

心跳检测技术是故障检测的关键技术之一。准确、高效的心跳检测机制是实现系统故障容错的基本条件。文献[6]通过限制心跳信息包的重发次数、可变的心跳参数以及增加对服务应用的侦测等策略，改进了传统的心跳检测技术的不足。文献[7-8]针对集群高可用领域，提出了通过调整心跳信息发送时间间隔来适应不同的网络状况。文献[9]针对单个主节点和多个从节点情况提出了一种分布式心跳协议，节点的心跳过程相同且处于不同的状态。本文以三重化冗余ETS系统为研究对象，着重研究了多个主节点和多个从节点的多机环境下的心跳检测机制，对各控制器间存在的主从关系作进一步探讨，以减少通信开销，提高检测实时性。

1 系统结构与原理

三重化冗余ETS系统主要包含智能输入模块、主控制器、总线控制器和智能输出模块，采用带隔离的满足CAN 2.0B规范的高速CAN总线作为模块间的传输总线。系统输入、数据传输、决策控制、

收稿日期：2008 – 10 – 20；修回日期：2009 – 02 – 16
基金项目：部级预研基金(51317030306)
作者简介：邹见效(1978 –)，男，博士，副教授，主要从事智能信息处理与控制方面的研究.

系统输出等主要模块采用物理上无耦合、分离式结构的三重化设计。通过3取2表决机制提高系统的可靠性和安全性，系统主要模块具备自测试功能，可在不中断系统运行的情况下更换部件。系统结构如图1所示。由图可知，3条独立的总线α、β、γ连接3组无耦合的输入模块、总线控制器、输出模块。每个主控制器通过3个总线控制器与该3条总线相连。如主控制器A，通过总线控制器Aα与总线α相连，通过总线控制器Aβ与总线β相连，通过总线控制器Aγ与总线γ相连。每个主控制器通过另外的CAN总线与它对应的3个总线控制器相连。输出模块实现输出信号的3取2表决及对输出负载的驱动。图1中的负载为危急跳闸系统的跳闸电磁阀，系统输出为多组跳闸电磁阀的开关量控制信号。

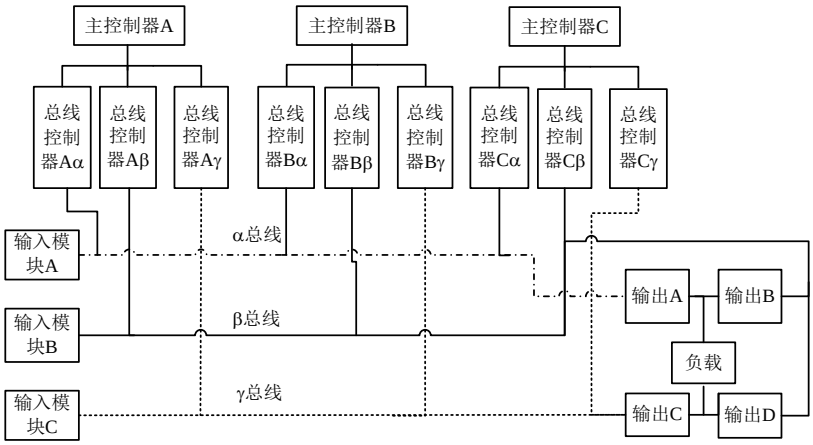

图1 系统原理框图

主控制器主要实现三冗余ETS系统的输入信号表决、偏差报告、应用程序处理、故障诊断、自测试等功能。总线控制器主要完成输入、输出模块与主控制器之间的数据转发。输出模块实现输出信号的表决及对输出负载的驱动。输入、输出模块均设计为单个模块16个I/O点。

下面的讨论根据某300 MW火电机组要求，以输入、输出模块均配置64个I/O点的系统为研究对象。系统单条总线上的节点有4个智能输入模块、3个总线控制器、4个智能输出源模块、4个智能输出受控漏模块，一共有3条总线。3个主控制器都需获取3条总线上所有模块的存活信息，以便作出正确的数据表决及处理。

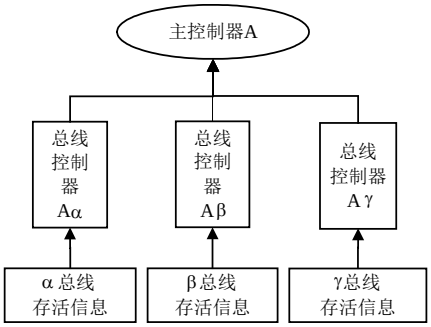

图2 三冗余模块失效检测通信关系

以主控制器A为例，它连接的3个总线控制器Aα、Aβ、Aγ分别属于3条总线α、β、γ，每个总线控制器把其所在总线上的模块存活信息汇总后，再发送给主控制器，其失效检测通信关系如图2所示。

以总线α为例，总线控制器Aα需要汇总总线控制器Bα和Cα、输入模块α、输出模块α、受控漏模块α的存活信息。其失效检测通信关系如图3所示。

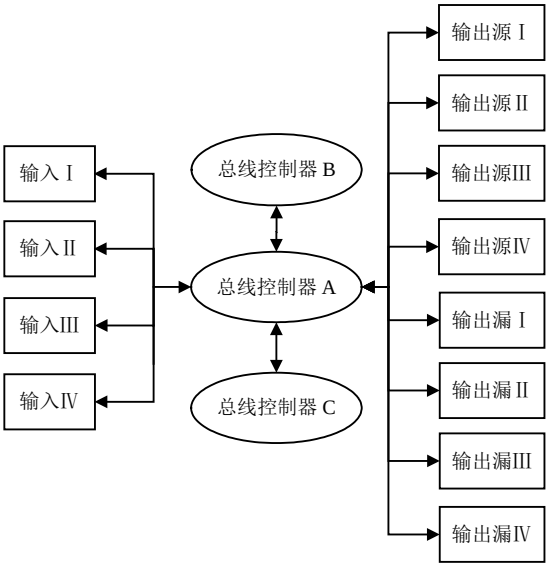

图3 单条总线中总线控制器A与其他模块通信示意图

2 心跳检测方法的改进

心跳检测方法按照其实现模式的不同，可以分为PUSH和PULL两种模式[10-12]，二者都是通过周期性地发送检测信息检测对方的状态(是否已经发生

失效)。所不同的是，PUSH模式是被检测对象主动向它的检测对象周期性地发送PUSH心跳信息，而PULL模式则是由检测对象向被检测对象发送查询信息，而被检测对象收到查询后，被动地发回应答信息。

为方便讨论，假设检测对象与被检测对象之间的单次通信开销均相同，即通信数据包占用总线通信时间相同，定义为f。总线上其他模块个数为14。

如果采用PULL模式，则每检测一次就需要总线控制器A向总线上模块发送查询信息，总线上模块收到后回应应答信息，双方交互一次，通信开销较大，为：

$$F_{\mathrm{PULL}} = 28f \tag{1}$$

如果采用PUSH检测模式，则需要总线上模块向总线控制器发送心跳信号，通信开销为：

$$F_{\mathrm{PUSH}} = 14f \tag{2}$$

PUSH模式下，总线控制器A在一个周期内没有收到总线上模块的心跳信号，就会判定总线上的某个模块失效，但是该心跳信号可能是由于延迟没有及时到达，易造成误判，可能导致很严重的后果。

2.1　PUSH结合PULL心跳检测方法

为了满足系统的要求，提高模块失效判别准确率，减少系统通信开销，系统采用将PUSH和PULL两种检测模式相结合的检测方法。在总线控制器Bα和Cα、输入、输出、受控漏模块中采用PUSH检测机制，设置PUSH心跳信号的时间间隔为T_1，各总线模块主动向总线控制器Aα发送PUSH心跳信息。在总线控制器Aα设置PULL检测机制，假设PULL检测时间周期为T_2，且$T_2 > T_1$，即PULL检测的时间周期要比PUSH检测的时间周期长。PULL检测模式利用定时器定时，如果在一个时间周期T_2内收到所有总线上模块的PUSH心跳信号，则定时器进入下一个定时周期；如果在一个周期内没有收到某个总线模块的PUSH心跳信号，则定时器激活总线控制器Aα，对该模块进行一次PULL检测，判断它是否失效。如果在下一个时间周期T_2内没有收到该模块的PULL响应信息和PUSH心跳信号，则认定该模块失效。

为了检查在一个周期T_2内总线控制器Aα是否收到总线上各个模块的心跳信号，在总线控制器Aα上设置一个记录各个模块心跳信号的存活状态列表。初始状态，每个模块的值都为0，如果收到了PUSH心跳信号，则相应位置1。当时间到达T_2时，总线控制器Aα通过查看状态列表，向状态值为0的模块发送PULL检测信号。如果收到该模块的PULL响应信号，则修改状态列表的值为1；如果没有收到，则确定其失效。总线上其他模块的状态如表1所示。

表1　总线上各模块的存活状态表

模块名称	α输入Ⅰ	α输入Ⅱ	α输入Ⅲ	α输入Ⅳ	α源输出Ⅰ	α源输出Ⅱ	α源输出Ⅲ
状态	0	1	1	1	0	0	0
模块名称	α源输出Ⅳ	总线控制器Bα	总线控制器Cα	α受控漏输出Ⅰ	α受控漏输出Ⅱ	α受控漏输出Ⅲ	α受控漏输出Ⅳ
状态	1	0	0	1	1	1	1

假设总线控制器在一个给定时间内没有收到总线上其他模块心跳信号的概率为p。在一次检测过程中，i个总线模块的心跳检测信号没有到达总线控制器Aα的概率满足二项分布，为：

$$P(\zeta = i) = C_{14}^{i} p^{i} (1-p)^{14-i} \tag{3}$$

式中　$0 \leqslant i \leqslant 14$，且$i$为正整数。本文系统中，每个时间周期内，单条总线上所有14个模块的PUSH心跳信号的平均不到达率为：

$$E(P) = \sum_{i=0}^{14} i C_{14}^{i} p^{i} (1-p)^{14-i} \tag{4}$$

如果没有收到PUSH心跳信号，则总线控制器Aα会发起PULL检测。所以在一次完整检测过程中，PULL检测的通信开销为：

$$F_{11} = 2fE[P] = 2f \sum_{i=0}^{14} i C_{14}^{i} p^{i} (1-p)^{14-i} \tag{5}$$

因此，在PUSH结合PULL检测模式下，总的通信开销为：

$$F_1 = F_{\mathrm{PUSH}} + F_{11} = 14f + 2f \sum_{i=0}^{14} i C_{14}^{i} p^{i} (1-p)^{14-i} \tag{6}$$

因为$0<p<1$，由计算可得 $\sum_{i=0}^{14} i C_{14}^{i} p^{i} (1-p)^{14-i} < 1$，则：

$$F_{\mathrm{PULL}} - F_1 = 14f - 2f \sum_{i=0}^{14} i C_{14}^{i} p^{i} (1-p)^{14-i} > 0 \tag{7}$$

PUSH结合PULL的模式比只使用PULL的模式降低了通信开销，比只使用PUSH的模式降低了误判率，提高了系统故障检测的可靠性。在该模式下，采用的是集中检测模式，当总线上模块数量较多时，总线控制器Aα需要监测所有总线上节点的存活状态，负担较重。对于三冗余系统，输入模块、总线控制器、输出模块之间的通信量已经很大，如果再加上多节点的心跳检测，有可能导致数据冲突，因为模块失效而影响系统的正常通信。

2.2　分级检测方法

为减少总线上同时进行心跳检测的节点数，根

据三冗余系统的特点，以及各控制器在系统的不同作用，引入分级心跳检测机制。

在检测机制上作如下定义：4个16路输入模块定义为一个主输入模块和3个从输入模块，即从模块通过主模块与总线上的其他模块进行交互；输出源模块和受控漏模块也定义成主从关系，即4个输出源模块定义为主模块，4个受控漏模块定义为从模块。在总线控制器Aα中设置PULL检测机制，存活状态列表中只记录总线控制器Bα和Cα以及主输入模块、输出源模块的存活状态。在从输入、从输出中设置PUSH检测机制，定时向主输入、主输出发送心跳信号。主输入、主输出不仅要定时向总线控制器Aα发送自身的PUSH心跳信号，还要检测它们的从输入模块、受控漏模块的存活状态，如果发现从输入模块、受控漏模块失效，则向总线控制器Aα报告。在分级检测模式下，总线控制器Aα与总线上模块的通信关系如图4所示。

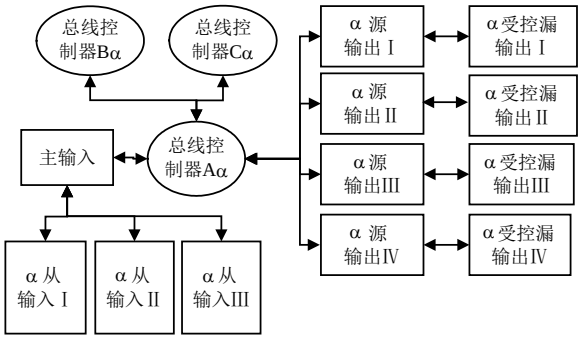

图4 单条总线控制器Aα与其他模块失效检测关系

本文模式中，直接发送PUSH心跳信号给总线控制器Aα的模块个数为7，总线控制器与主输入模块、主输出模块之间进行一次完整检测(PULL和PUSH检测)的通信开销为：

$$F_{21} = 7f + 2f\sum_{i=0}^{7} iC_7^i p^i (1-p)^{7-i} \tag{8}$$

从输入模块、受控漏模块发送PUSH心跳信号给主输入模块和输出源模块的检测通信开销为：

$$F_{22} = 7f \tag{9}$$

则整个检测机制的通信开销为：

$$F_2 = F_{21} + F_{22} = 14f + 2f\sum_{i=0}^{7} iC_7^i p^i (1-p)^{7-i} \tag{10}$$

$$F_1 - F_2 = 2f[\sum_{i=0}^{14} iC_{14}^i p^i (1-p)^{14-i} - \sum_{i=0}^{7} iC_7^i p^i (1-p)^{7-i} > 0 \tag{11}$$

由式(11)可知，加入分级检测模式，总的检测开销比使用PULL结合PUSH方法降低了，并且减轻了总线控制器的检测负担。

2.3 心跳检测融入数据传输模式

在系统的模块失效检测中，判断其存活与否，关键是看是否收到PUSH信号以及PULL检测是否收到响应信息。在输入、输出中设置PUSH机制，直接把输入、输出模块发送的数据作为其PUSH信号，而不专门定义和添加PUSH信息包，即把正常的周期性数据传递认为是PUSH心跳信息，就可以既不影响系统正常的数据传输，又可以实时地进行模块失效检测。

加入主从检测后，主输入、输出模块每次发送心跳信号时都把从输入模块、受控漏模块的失效信息包含到心跳信息里，则总线控制器就能实时了解从输入模块、受控漏模块的存活状态，并且不用主输入、输出模块再重新发送一次从输入模块、受控漏模块失效的信号。设从输入模块、受控漏模块发送给主输入、输出模块的PUSH信号的时间周期为T_c，为保证主输入、输出模块每次发送给总线控制器的心跳信号中都包含正确的从输入模块、受控漏模块的存活状态，则主输入、输出模块发送给总线控制器的PUSH信号时间周期T满足$T > T_c$。

在这种模式下，PUSH信号的通信开销已经成为系统正常开销的一部分，不计入模块失效检测开销中，而唯一的开销是当总线控制器Aα没有收到总线上其他模块的PUSH信号时，发出的PULL检测，总通信开销为：

$$F_3 = 2f\sum_{i=0}^{7} iC_7^i p^i (1-p)^{7-i} \tag{12}$$

由式(1)、式(6)、式(10)、式(12)比较得知：把心跳检测融入数据传输模式下，系统模块失效检测的通信开销最小，并且由于结合了PUSH和PULL检测，使用了分级检测方法，满足了三冗余系统对模块失效检测方面的可靠性、实时性、通信开销小的要求。

3 系统仿真与现场调试

3.1 通信开销仿真

由式(1)、式(6)、式(10)、式(12)可知，只使用PULL、结合PULL和PUSH、加入分级检测、心跳检测融入数据传输这4种模式的通信开销分别为F_{PULL}、F_1、F_2、F_3。假设总线控制器Aα在一定时间内没有收到总线上模块心跳信号的概率p为0.01，则利用Matlab仿真各种模式下的单位通信开销f与总通信开销F的结果如图5所示。

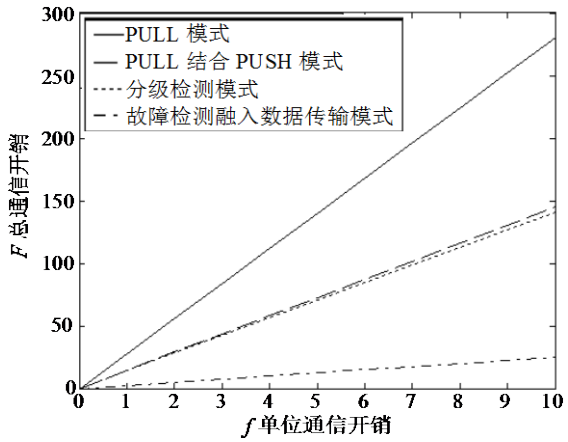

图5　各种模式下单位通信开销与总通信开销的仿真结果

由图5可知，在相同的单位通信开销下，结合PULL和PUSH模式、加入分级检测模式和心跳检测融入数据传输模式对于心跳检测的改进，大大降低了通信开销。改进的心跳检测机制比只用PULL模式降低了通信开销，比只用PUSH模式提高了判断的正确率。在保证模块失效检测的可靠性与实时性的前提下，不占用过多的系统通信资源，满足三冗余系统在线实时模块失效检测的要求。

3.2　系统现场调试

三冗余ETS系统调试环境如下：输入、输出智能模块每个模件采用16个I/O点设计，通过组合4个模块构成输入、输出均为64点的系统，模件之间采用背板方式相互连接并装入机柜。试验系统控制逻辑采用某300 MW汽轮机发电机组ETS系统要求。该系统经过长期通电试验，并反复进行了总线通信及故障检测的测试，能快速并正确地判断出总线模块故障，心跳检测方法在系统中运行良好，其稳定性得到证明。

4　结　论

以汽轮机三重化冗余危急跳闸系统为研究对象，针对可靠性和实时性要求较高的多机系统，研究并设计了多主多从结构的多机环境下高可靠系统的心跳故障检测机制。结合PUSH和PULL模式的检测方法，并采用主从检测及将心跳检测信息融入系统数据的措施，减少了用于系统故障监测的通信开销并减小了误判率。通过在某300 MW的汽轮机危急跳闸系统的现场应用，证明了该方法的可行性与可靠性。该心跳检测机制也可扩展到其他应用场合。

参　考　文　献

[1] 中华人民共和国电力工业部. DL/T596-1996 电力设备预防性试验规程[S]. 北京: 中国电力出版社, 1997.
Ministry of Power Industry of Peopler's Republic of China. DL/T596-1996 Preventive test code for electric power equipment[S]. Beijing: China Electric Power Press, 1997.

[2] 何湘杰, 张　静. PLC在汽轮机ETS系统中的应用研究[J]. 汽轮机技术, 2005, 47(3): 225-226.
HE Xiang-jie, ZHANG Jing. Study on application of PLC to ETS system of steam turbine[J]. Steam Turbine Technology, 2005, 47(3): 225-226.

[3] 曾广商, 沈卫国. 高可靠三冗余伺服机构系统[J]. 航天控制, 2005, 23(1): 35-40.
ZENG Guang-shang, SHENG Wei-Guo. High-reliability triple redundancy servo mechanism system[J]. Aerospace Control, 2005, 23(1): 35-40.

[4] 王丽华, 徐志根, 王长林. 可维修三模冗余结构系统的可靠度与安全度分析[J]. 西南交通大学学报, 2002, 37(1): 103-107.
WANG Li-hua, XU Zhi-geng, WANG Chang-lin. Reliability and security analysis of 3-module redundancy system with one maintainable unit[J]. Journal of Southwest Jiaotong University, 2002, 37(1): 103-107.

[5] CHEN Guang-yu, Huang Xi-zi, Tang Xiao-wo. Analysis of phased-mission system reliability and importance with imperfect coverage[J]. Journal of Electronic Science and Technology of China, 2005, 3(2): 182-186.

[6] 吴书华, 吴庆波, 张　超. KylinOS可靠心跳协议研究[J]. 微计算机信息, 2006, 22(11-2): 52-54.
WU Shu-hua, WU Qing-bo, ZHANG Chao. The research of KylinOS reliable heartbeat protocol[J]. Microcomputer Application, 2006, 22(11-2): 52-54.

[7] 谢长生, 胡庆平, 谭志虎. Heartbeat-Gear: 一种新型的实时心跳监测技术[J]. 计算机工程与科学, 2006, 13(6): 59-61.
XIE Chang-sheng, HU Qing-ping, TAN Zhi-hu. Heartbeat-Gear: a new real-time heartbeat inspecting technique[J]. Computer Engineering and Science, 2006, 13(6): 59-61.

[8] WAN Ya-ping, FENG Dan, YANG Tian-ming, et al. The adaptive heartbeat design of high availability RAID dual-controller[C]//2008 International Conference on Multimedia and Ubiquitous Engineering. Seoul, Korea: [s.n.], 2008: 45-50.

[9] HOU Zong-hao, HUANG Yong-xiang, ZHENG Shou-qi, et al. Design and implementation of heartbeat in multi-machine environment[C]//Proceedings of the 17th International Conference on Advanced Information Networking and Applications. Xi'an, China: [s.n.], 2003: 583-586.

[10] SOTOMA I, MADEIRA E R M. Adaptation-algorithms to adaptive fault monitoring and their implementation on CORBA[M]. Rome: IEEE Computer Society Press, 2001.

[11] CHAZAL P de, DWYER M O, REILLY R B. Automatic classification of heartbeats using ECG morphology and heartbeat interval features[J]. IEEE Transactions on Biomedical Engineering, 2004, 51(7): 1196-1206.

[12] JOHNSON T, MUTHUKRISHNAN S, SHKENYUK V, et al. A heartbeat mechanism and its application in gigascope[C]//Proceedings of the 31st International Conference on Very Large Data Bases. Trondheim, Norway: [s.n.], 2005: 1079-1088.

编　辑　漆　蓉