能量管理系统的不间断故障切换方法

张良栋
(广东电网公司 韶关供电局,广东 韶关 512026)

摘要: 能量管理系统(EMS)的主设备的硬件或软件系统出现故障时,就会执行主、备设备的故障切换。在对 EMS 故障切换全过程时间进行分析后,确定侦测时间段是影响故障切换时间的主要因素。提出在系统侦测时段中适当选取判定次数(3~5 次)和执行间隔(100~400 ms)的可变间隔的侦听程序方法可缩短故障切换时间(可控制在 3 s 内)。提出在通信中对关键性报文采用流水编号及断点报文重传的方法,保证了 EMS 的良好运行。

关键词: 能量管理系统; 故障切换; 侦测时间段; 不间断
中图分类号: TM 76;TN 919 **文献标识码**: B **文章编号**: 1006-6047(2005)09-0083-03

0 引言

为了提高能量管理系统(EMS)[1~4]的可靠性[5],系统中的前置、后台处理机,通信处理机等关键设备都采用冗余配置。通常冗余配置的设备构成互为热备用运行模式[6],"主""备"机的切换分为人工切换和自动切换 2 种。自动切换又分为正常切换和故障切换 2 种,正常切换通常只为了延长设备使用寿命,让主、备设备按预定时间切换交替使用;而故障切换是硬件或软件系统出现问题后系统不得不采取的行动。

就处理机而言,故障切换过程可能造成系统对信息收集、处理的短时间"真空","真空"期间可能造成实时信息丢失,从而对系统性能造成伤害,"真空"时间越短,伤害越小,反之越大。为此有关 EMS 国家标准[7]中对处理机故障切换时间做了规定(≤30 s,各级电网运行部门的技术规范中也对此提出了更具体的要求。目前国内不同 EMS 产品的这一技术指标存在较大的差异(从 3~30 s,甚至更长)。本文根据对故障切换全过程的分析,以及从事 EMS 设计的经验,介绍了处理机故障切换判断和实现方法,可以将故障切换时间大大缩短。

收稿日期:2005-05-12;**修回日期**:2005-06-27

1 故障切换时间分析

故障切换的全程时间从主机出现故障算起,到后备机接替工作成为新的主机并在界面上显示告警为止。如图 1 所示,故障切换时间包含 4 个时刻:主机发生故障时刻 t_0;后备机获知主机故障,发出告警并开始接替工作时刻 t_1;后备机完全接替主机工作并宣布成为新的主机时刻 t_2;人机界面显示出切换告警信息时刻 t_3。它们构成 3 个时间段:侦测段 $t_{01}=t_1-t_0$;接替段 $t_{12}=t_2-t_1$;显示段 $t_{23}=t_3-t_2$。由于 t_2 后系统功能已经恢复正常,所以有观点认为故障切换过程可不包括 t_{23},但笔者认为 t_{23} 时间段内,告警等需要现场处理的信息仍然无法及时处理,所以应该将其计算在内。故障切换时间示意图见图 1。

Research on DSP-based protective device for mid/low-voltage power system

ZHANG Ren-yin[1], XIA Jin-sheng[2]
(1. Zhangzhou Electric Power Bureau, Zhangzhou 363000, China;
2. Guodian Nanjing Automation Co., Ltd., Nanjing 210003, China)

Abstract: The development of DSP-based integrated measuring and protective device for mid/low-voltage power system is studied, including the protection theory, the design, manufacturing and commissioning of hardware system, and the systematic design of its configuration. Modules of the modularized and unified hardware system are emphasized, including central processing, man-machine interface, A/D conversion, outlet, communication, frequency and phase measuring, and so on. The designed and implemented functions of each module are analyzed, and the improvement of anti-interference capability is discussed.

Key words: microcomputer-based measuring and protective device; digital signal processor; modularization

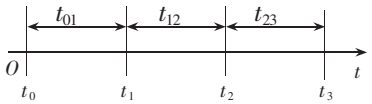

图1 故障切换时间示意图

Fig.1 Time of fault switching

在侦测时间段 t_{01} 中,主机发生的故障主要有3种情况:计算机故障;网络通信故障;预定义的重要任务(应用软件)故障并连续自举失败达到规定次数。发生前2种情况时,由后备机"侦听"发现故障;发生第3种情况时由主机主动告知后备机,不依靠侦听。通常的侦听实现方法是,互为备用的2台(或1组)计算机上对等配备1个侦听程序,以设定的频度相互交换"心跳"信息,当后备机连续超过设定次数不能获得主机"心跳",判断为对方发生故障。因此该时间段由3个因素决定:通过局域网进行1次"心跳"信息交换所需时间 t(单位 ms);侦听程序执行间隔 t_{Iint}(单位 ms);连续"停跳"次数 m(判定同伴为故障的依据)。当 t_{Iint} 为固定值时侦测时间段 t_{01} 与三者的关系可表示为

$$t_{01}=m(t+t_{\mathrm{Iint}}) \tag{1}$$

当 t_{Iint} 为可变值时 t_{01} 与三者的关系可表示为

$$t_{01}=t+t_{\mathrm{Iint0}}+(m-1)(t+t_{\mathrm{Iint1}}) \tag{2}$$

式中 t_{Iint0} 为初始间隔;t_{Iint1} 为变化后的间隔。

在接替时间段 t_{12} 中,系统需要完成以下的操作。

a. 系统管理数据库中原后备机和原主机的状态对调,并通过网络向分布系统中相关的设备发布消息,不论是采用"可靠广播"还是采用点对点通信方式,这一过程所需的时间一般不超过几十毫秒(一般系统中的节点数仅几十个)。

b. 原后备机取代原主机的工作,如果原后备机处于完全的热备用状态,只需将任务本身定义为"值班",所花时间可以忽略;即使原后备机处于不完全热备用状态,激活处在不活动状态的任务(一般由应用软件实现)所需时间也是毫秒级的。

由此可见时间段 t_{12} 至多不过几十毫秒。

显示时间段 t_{23} 取决于人机界面软件对待事件的响应逻辑及响应速度。主机发生故障切换应列为系统较重大事件,所以切换告警和切换完成的信息应立即推出窗口告诉操作人员,以目前计算机处理速度,人机界面软件推出告警窗口的时间(即 t_{23})一般不会超过1 s。

2 控制故障切换时间的方法

根据以上分析,故障切换的3个时间段中,接替时间段 t_{12} 占比重很小,显示时间段 t_{23} 对于具体应用程序基本是固定的,要想缩短故障的切换时间,可供挖掘的潜力主要是侦测时间段 t_{01}。下面通过分析式(1)中3个自变量说明如何控制故障切换时间。

a. 可人为设定连续"停跳"次数 m,因为 t_{01} 与 m 成正比,因此 m 不宜过大;但为了避免因偶然的通信延误产生误判,m 也不宜等于1。一般设定为3~5。

b. 可人为设定侦听程序执行间隔 t_{Iint},设定的原则是在不过于消耗CPU和网络资源的前提下选择尽可能小的间隔,一般在200~400 ms间选取。这样的执行频度不会消耗过多的CPU和网络资源,因为侦听程序每次需要完成的工作基本上只是一个小报文通信过程。

c. 进行1次"心跳"信息交换所需时间 t,理论上说2台计算机交换1次心跳的时间与局域网负载水平有关,但是对合理分布的EMS系统以及目前常用的100 Mb网络,EMS局域网正常负载水平不会超过15 %,在这样负载条件下,根据实测利用一个小报文通信过程交换1次心跳的时间 t 约需1 ms。与间隔 t_{Iint} 相比,显然 t 可以忽略不计;这样式(1)(2)可分别简化为

$$t_{01}=m\,t_{\mathrm{Iint}} \tag{3}$$

$$t_{01}=t_{\mathrm{Iint0}}+(m-1)t_{\mathrm{Iint1}} \tag{4}$$

根据以上分析,当设定 $m=3$ 且 $t_{\mathrm{Iint}}=200$ ms时,按式(3)计算 $t_{01}<0.6$ s;当设定 $m=5$ 且 $t_{\mathrm{Iint}}=400$ ms时,则 $t_{01}<2$ s。

再看侦听程序采用可变间隔的情况,当设定 $m=3$ 且 $t_{\mathrm{Iint0}}=200$ ms,当第1次心跳交换失败后,侦听程序自动设定 $t_{\mathrm{Iint1}}=100$ ms,则按式(4)计算 $t_{01}<0.4$ s;当设定 $m=5$,$t_{\mathrm{Iint0}}=400$ ms时,第一次心跳交换失败后侦听程序设定 $t_{\mathrm{Iint1}}=100$ ms,这样 $t_{01}<1$ s。显然采用可变间隔可使 t_{01} 时段进一步缩短。由于故障是偶然发生的,采用可变间隔的侦听程序绝大部分时间会按设定的初始间隔执行,只是在故障情况下临时将侦听间隔缩短到100 ms,因此不会对CPU和局域网造成冲击。

总而言之,选取适当的判定次数 m 和执行间隔,将 t_{01} 控制在2 s甚至1 s以内是不难实现的,加上其他2个时段后总的切换时间可以控制到3 s甚至2 s以内。

3 不间断故障切换

理论上,即使将 t_{01} 控制到1 s以内,仍然消除不了信息收集和处理的真空阶段。如果不采取其他手段,就无法完全避免故障切换对系统的影响。

采用无缝切换技术或容错计算机是实现不间断故障切换的方式之一,但这种方式经济上代价较大,一种既实用又简单的方法是在通信过程中实现"断点重传"功能。

如图2所示,实现断点重传有下面4点功能。

a. 对传送实时数据的报文设置序号,该序号一般是连续的流水号,并保证比较长的一段时间内不重复。这样,当故障切换后,新主机接收到的报文序号出现"跳号"时,新主机可以根据报文序号判断出在故障切换过程中是否丢失了报文,以及丢失的具体是哪些报文。

b. 故障切换后,新主机根据需要判断是否丢失报文,如果丢失了报文,新主机首先找出丢失报文的序号,并根据序号的先后顺序,逐一向发送者发送要求重新上传报文的请求。

c. 发送者接收到新主机重新上传报文的请求,根据报文序号重新发送相应的报文。

d. 新主机接收到断点重传的信息,可以根据报文的序号将报文内容插入到本地存储区中,也可以将重传的信息直接排在已经接收信息的后面,并由应用程序排序并使用。

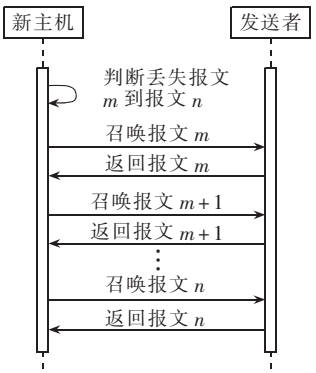

图 2 新主机召唤序列图

Fig.2 Sequence of new master polling

这种实现方式要求发送者暂时保存发送过的报文,需要缓存的报文数量随 t_{01} 而定,假如 t_{01} 在 2 s 以内,只需要暂存最近发送的 1 个报文就行。否则随 t_{01} 延长,需要暂存的报文数量将增加,这时发送者缓存区要增加,而且处理工作量也随之增加。因此,断点重传功能的实现可以和控制故障切换时间的方法结合使用。

4　结语

减少故障切换时间,是提高能量管理系统可靠性的关键之一。本文提出了一种可变间隔的故障侦听方法,可以使 EMS 处理机故障切换时间缩短到 3 s 甚至 2 s 以内。同时,本文提出了一种报文重传的方法,与可变间隔的故障侦听方法结合使用,可以避免故障切换造成的数据丢失,保证了 EMS 的实时、安全、稳定、可靠。

参考文献:

[1] 于尔铿,刘广一,周京阳. 能量管理系统(EMS):第一讲 EMS 的技术发展[J]. 电力系统自动化,1997,21(1):65-68.
YU Er-keng,LIU Guang-yi,ZHOU Jing-yang. Energy management system(EMS):Part one technical evolution of EMS [J]. **Automation of Electric Power Systems**,1997,21(1):65-68.

[2] Draft IEC61970,Energy management system application program interface(EMS-API)part 301:Common information mode(CIM)base[S].

[3] Draft IEC61970,Energy management system application program interface(EMS-API)part 401:Component interface specification framework revision 4.1[S].

[4] Draft IEC61970,Energy management system application program interface(EMS-API)part 404:High speed data access reversion 2[S].

[5] 柏松山,韦　东,花思洋. 基于多重冗余技术的企业电力调度自动化系统[J]. 电力自动化设备,2004,24(12):46-48.
BAI Song-shan,WEI Dong,HUA Si-yang. Power dispatch automation system based on multi-redundancy technology [J]. **Electric Power Automation Equipment**,2004,24(12):46-48.

[6] 何　卫,马新平,张　焱,等. 变电站自动化分布式通信控制系统的设计[J]. 电力系统自动化,2000,24(16):48-50.
HE Wei,MA Xin-ping,ZHANG Yan,*et al*. Design of distributed communication control system in intergrated substation automation system[J]. **Automation of Electirc Power Systems**,2000,24(16):48-50.

[7] DL 5003-91,电力系统调度自动化设计技术规程[S].

(**责任编辑**:汪仪珍)

作者简介:

张良栋(1974-),男,广东韶关人,工程师,硕士,从事电力及其自动化系统专业技术研究和管理工作(**E-mail**:zhangdfh@sina.com)。

Bumpless fault switching in EMS

ZHANG Liang-dong

(Shaoguan Power Supply Company,Guangdong Power Grid Corporation,Shaoguan 512026,China)

Abstract: Fault switching between master and standby devices will be implemented when fault occurs in master devices of EMS(Energy Management System). Fault switching is analyzed from the view of execution time,and the detection time is considered as the main influencing factor. By properly selecting the judgment times(3~5) and implementation interval(100~400 ms) during detection process,an interval-alterable detection method is presented to shorten fault switching time within three seconds. For bumpless fault switching,the important messages should be identified with serial number and the interrupted telegraphs re-transmitted.

Key words: EMS; fault switching; detection time; bumpless