管理信息系统的容错设计技术

张莉　刘锋　（北京交通大学自动化所　100044）

摘要：本文以铁道部编组站管理信息系统（YIS）为例，并从系统平台结构和应用软件两方面来探讨容错设计技术，以此提高系统的可靠性。这种技术也可推广到其他类型的管理信息系统上。

关键词：容错　系统平台

一、前言

在信息高速发展的今天，管理信息系统已在各行各业得到了广泛应用。同时，又因为管理信息系统软件组成和硬件配置的复杂性，使其无论在设计上还是在维护上都有相当大的难度，在确保系统的可靠性方面尤其如此，因此容错设计技术在系统功能的实现具有重大意义。

二、容错设计技术的方法

容错设计技术的基本思想是通过对系统结构、设备配置、系统软件配置、应用软件等各方面加以备份或并行设计来屏蔽故障，从而保证系统正常运行的影响。

容错的方法有两种，一种是软件容错，其主要是通过多重软件设计可恢复模块结构等方式来实现；另一种是系统平台容错，其主要是通过在系统中加入冗余硬件及相应错误处理软件来实现。

操作系统和大型数据库容错属于系统软件容错，主要是采用了多处理器和特别设计的操作系统来达到容错并采用检查点的恢复机制。

本文将以铁路编组站管理信息系统为例着重研究系统结构容错和应用软件容错的设计技术。

三、系统结构容错

系统结构容错也为网络结构容错，网络容错应具备网络物理链路的连通性，网络接口板的高可靠性等。即要有能够检测故障的及其范围，并通过网络重构来隔离故障以及故障的恢复等特点。

为了便于问题的讨论，这里仅考虑总线型局域网，并以编组站管理信息系统为例，其网络结构如图 1 所示，其容错设施有：

(1)主机采用双机系统，两台主机互为备用，且可相互切换。

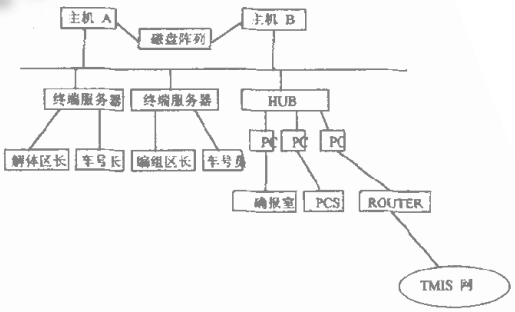

图 1　编组站管理信息系统结构图

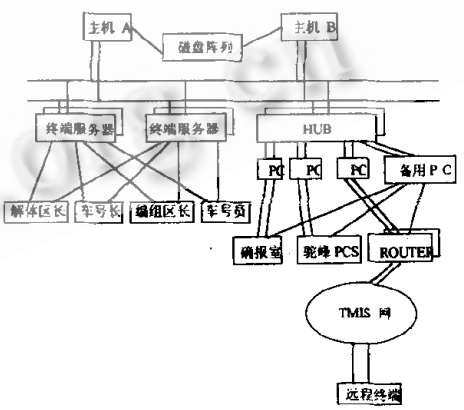

图 2　编组站管理信息系统容错网结构

(2)两台主机间配接公用磁盘阵列 7137，采用双电源供电连接 8 只高密磁盘，通过系统设置自动进行磁盘数据镜象工作。

在发生线路中断或通信器件发生故障时，网络原来容错设施仍会造成信息丢失，因此需要对网络线路及通

信器件进行容错设计经改造过的容错网如图 2 所示。具体容错方法如下：

1. 硬件容错

(1)采用双网工作方式。任何时刻只有一个网(如 A 网)处在通信工作状态，而另一网(如 B 网)处于备份工作状态，备份工作状态是指处于通信工作状态，只是尚无数据发送和接收而已，这样作的目的是为了考虑故障出现时便于诊断和隔离及网络的重构，且网络的有关软件仅有一套，这样，结构配置即使是双网结构，而用户使用网络时感觉到仍然是单网在工作，用户关心的数据能否准确及时的到达接收方，只有当某一网络出现故障时，他才被告知并在适当的时候进行网络电缆，板件或器件的替换工作。

(2)终端服务器、HUB、ROUTER、MODEM 或基带都备有冗余器件。冗余器件都处于备用状态，当器件发生故障后，备用器件将被自动切换，原器件将会热修复；

(3)对于重要终端用户，即影响现场作业的用户，如解体区长，车号长，信号员等等，每个用户分别与两个设置不同的终端服务器连线，即使一个终端服务器发生故障，也不影响现场作业；

(4)对于重要接口，如与确报接口，与 TMIS 的接口以及与驼峰 PCS 的接口，它们至主机的线路都有冗余，且网卡也有备份，线路和网卡都可以自动切换和热修复。

(5)设有远程终端，至远程终端的线路冗余且可自动切换。

2. 网络软件的扩充

由于我们是对现有的局域网加以改装来构成容错局域网，因此软件的扩充是必不可少的。总原则是保留原有的单网软件的所有功能，并在此基础上增加新的功能模块，尽可能独立于原有的功能模块，做到只有在需要切换时才调用这些功能，此外扩充的功能尽量在网络结构的低层实现，对上层软件越透明越好，感觉不到物理层是双份的最好。

因铁路编组站管理信息系统采用的是以太网，根据以太网的结构，我们知道在 MAC 层，可以得到以太网帧的数据。通过 IP PACKET 提供网络层相应数据在 MAC 子层和网络层可以进行地址的赋值和实现。同时，只有 MAC 子层能区分来自不同网络总线的数据，还可以直接填入用户数据，用 UDD 方式发送，所以必须在 MAC 子层和网络层进行编层，实现管理信息系统中的通信才具有较高的效率。具体实现过程如下：

(1)网络驱动程序的扩充。用一驱动程序驱动网板，并为上层软件提供相应的网板访问端口，因此首先要给两个网卡分配不同的端口基地址和设定各网卡的中断级别(或者决定查询的次序)。对于驱动程序报告的各种网卡出错信息进行分析，捕获哪些报告物理部件出错的信号，将其相应的出错信息报告给上层软件决定是否切换。

(2)协议软件的扩充。各种网络协议都是为了确保数据在网络上有效地可靠地进行传送。因此实现双网在其中一个故障时能顺利地切换到备份网以及后来故障网恢复到系统中。还有双 ROUTER，双终端服务器，双 HUB 之间的切换都需增加一些约定，这些约定就构成了要扩充的软件，通过诊断站诊断然后将故障汇报给主机，主机发送广播信息给各站点，(终端服务器，HUB，ROUTER)，通过主机的驱动程序进行自动切换。还需故障恢复后的检查信息。这些约定对完成切换及恢复是不可缺少的实现，这些约定的软件对用户是透明的。

以上思路及设计方法同样可用到广域网。

就可靠性而言，上述解决办法的基本思路是双倍冗余容错。这对于解决网络环境下数据可靠性问题，确实是一个行之有效的方案，然而却要用户付出双倍的代价去存储他们的数据和程序，尤其网络服务器往往采用高性能计算机系统，例如，对于多服务器应用环境，服务器镜像方案从代价上几乎是不可接受的，因此在硬件容错基础的同时，还需开发软件容错设计。

四、应用软件容错

软件容错设计除了操作系统和数据库容错设计外还有应用软件容错，通常在应用系统中，涉及容错功能开发的主要工作量是在应用系统中，同时应用软件也是最为关键的部分。

应用软件的设计思想是设置独立的容错模块并在设计编程时充分运用系统软件的容错技术。软件容错设计技术有自动检测、故障隔离、自动恢复等技术。编组站管理信息系统主要是 ORACLE7 关系数据库提供的 SQL * FORMS 工具软件开发的，因此容错设计要充分利用 ORACLE * FORM 特点来实现。本系统围绕容错主要采取以下措施。

1.设置监测模块,对错误进行定位

为了保障系统的正常进行,需要对系统的资源和运行状况进行监测和管理,通过监测,可对系统出现故障时,进行错误定位,并进行处理。编组站管理信息系统建立一个系统维护模块功能如下:

(1)系统性能监测

·监测 CPU 使用情况

·监测核心空间分配

·监测系统调用

·监测缓冲区

·监测终端

·监测对换和切换

·监测队列操作

·监测文件访问情况

·监测空闲内存

·监测进程间通信

(2)数据库性能监测

·调整内存:Library cache

·调整内存:Data Dictionary Cache

·调整内存:Database buffer Cache

·调整内存:Redolog Buffer

·调整 I/O:减少磁盘 I/O 竞争

·调整多线索调度进程的竞争

·调整响应队列的竞争

·调整请求队列的竞争

还有对现在库内容检查看虚实场字典是否有多余的东西。

2.充分利用系统工具

·在编制 form 时,设置 on - error on - message 触发子。如在 Runform 时发生错误可通过打开 On - error On - message 来对错误进行定位。

·利用 Oracle 提供的函数 Form - success 判别内部程序成功与否。

·利用 Oracle 提供的函数 SOLCODE, SOLERRM 判别程序执行过程中发生何种类型例外及对例外的说明。

·利用 Oracle 提供的函数 ERROR - TYPE, ERROR - CODE, ERROR - TEXT 获取 Oracle 给出的标准错误类型、错误代码以及具体错误解释信息。设置 CRTR + R 防止非异常关机,反复启动非正常状态下保证数据进程的完成与恢复,避免软件系统故障。

3.设置恢复功能,采用向后恢复法

对于大型软件系统,特别是管理信息系统,数据要求准确不误,恢复功能可防止操作人员的误操作,通过恢复进行修改,编组站管理信息系统采用的恢复技术(多采用的是向后恢复法)有:

·设置虚实作业场数据恢复功能

·设置钩计划预执行功能

·设置钩计划回推功能

·设置钩计划取消功能

·设置虚出发场的功能

注意:当编组区长模拟编车时,而出发场的车实际还为出库,虚出发场是防止车辆叠置所设的功能。

4.对数据字典进行多重保护,保证数据的完整性

在管理信息系统中,若数据字典部分被删除或被修改,有时会影响整个系统的正常运行,通过设置节点群,每个节点都知道群集中其他成员及分配给它们的应用程序包,一但一节点出现故障时,剩下的节点会将其从群集中去掉,以防止其访问磁盘,从而防止故障点对磁盘的写操作。

五、结束语

随着当今社会的信息化、建设长足发展,各类信息处理系统在经济、教育、科研、政府等各个方面得到了广泛的应用,而且增长速度远远超过了人们的预料。

在这个飞速增长的过程中,有两个趋势引起了我们的注意:一是信息系统规模越来越大,业务种类越来越复杂,许多信息处理系统在本行业全国范围内应用并具有中央处理的功能;二是许多行业信息处理系统的重要性越来越高,短时间的意外中断就会造成不可估量的损失。

在这种情况下,大型信息处理系统的容错设计技术必将得到越来越广泛的应用,因此将信息处理的容错技术系统化、完整化,使之成为信息系统设计的有机部分是很有必要的,本文在这方面做了肤浅的探讨,希望能起到抛砖引玉的作用,并希望得到有关专家的批评指正。

(来稿时间:1997 年 8 月)