硬件冗余在安全控制系统中的应用

范丽云　（北京理工大学计算机科学与工程系　100081）
武保红　（中国铁路通信信号总公司　100038）
黄维金　（中　国　人　民　公　安　大　学　100038）

摘要：硬件冗余是提高安全控制系统可靠性的一种常用技术手段。本文以一个实时采集控制模型，探讨安全控制容错技术中的关于硬件冗余的应用策略。

关键字：主机　备机　表决机　采集对象　控制对象　主机输出机制　并行输出机制　控制系统

本文基于计算机的可靠性，探讨硬件冗余在安全控制系统中的应用。

1. 多处理机间的多主体协作

提高计算机的可靠性，目前主要采用两类技术：

·避错技术——主要是防止和减少故障发生。可通过提高产品的质量，加强工艺控制，计算机系统工作的环境的保护和减少所带负载等措施来实现。这类技术要求工艺水平高，技术难度大，费用高。

·容错技术——当计算机系统的某一部分发生故障时仍使系统保持正常工作，而可靠性几乎没有降低。该技术手段往往是采用牺牲资源（如设备资源、时间资源和信息资源等）来换取系统的可靠性。

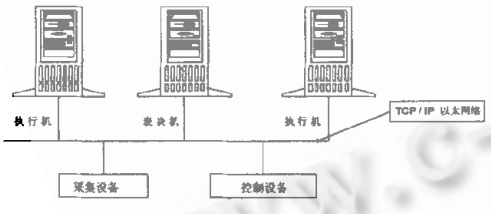

图 1　实时采集控制系统示意

目前在高可靠性系统中，广泛采取容错技术。容错技术在不同行业，基于不同的应用、不同的安全级别以及不同的设计者之间的系统设计千差万别，下面仅就实时采集控制中的一个应用模型，探讨安全控制容错技术中多处理机间的多主体协作问题。

为了便于说明，下面讨论三个处理机间的主机并行工作机制。图 1 是由两个执行机（执行机 A 和执行机 B）、表决机 C、TCP/IP 网络、采集设备和控制设备（也叫输出设备）组成的一个实时采集控制系统。其中的采集设备负责把采集到的现场信息传送给三台主机；三台主机通过一定的运算，把运算结果通过某种机制进行比较，然后根据预先设定的机制发送控制命令给控制设备；最后由控制设备对现场的控制对象进行控制。

图 1 中三台主机所负责执行的工作是相同的，即用相同的输入，各自进行运算后将结果通过某种方式进行“表决”，最终把表决结果送给控制设备，由控制设备对控制对象的输出进行控制。上述配置是典型的容错技术中的一个应用——硬件冗余。

三台主机用相同的输入（由输入设备采集到的现场开关量 0 或 1），当其中的一台主机对某一控制对象的计算结果和其他两台不一致时，采用“少数服从多数”的原则进行表决。即该主机对控制对象的计算结果“弃权”，采取“三取二”的机制将另两台主机的计算结果控制该控制对象。如果其中的一台主机发生故障（如硬件故障），该系统通过声音等手段进行报警，同时继续通过“二取二”进行正常工作。

图 1 中，对三台主机的输出结果进行比较可以有多种方式，下面仅介绍其中的两种输出计算机制——主机输出机制和并行输出机制。

2. 主机输出机制

在图 1 中，可以令执行机 A 和 B 同时具有输入和输出功能，但同一时刻只有 A 和 B 中的一台进行输出，我们称当前正在进行输出的执行机为“主机”；而另一执行机则为“备机”。表决机 C 只具有输入功能，不具备输出功能。表决机的运算结果只参与表决运算，当 A、B 执行机的运算结果不一致时，用表决机 C 的运算结果确定 A

和 B 谁成为主机进行输出。

其表决过程如下：

(1) 表决机 C 将运算结果分别传送给主机(当前具有输出权的 A 或 B 机)和备机(没有输出权的 A 或 B 机)；主、备机的运算结果则相互传送，主、备机同时进行“三取二”运算。若主机运行结果与另外两台主机的运行结果一致，则主、备机仍为原来的主、备机。

(2) 当某一执行机或表决机在出现硬件故障、网络故障、断混线故障和外界干扰引起的暂时运算错误等情况下，为了保证故障安全侧的正确输出，从而保证该安全控制系统的可靠运行。系统表决算法如下：

① 若表决机 C 故障，执行机 A 和 B 双机运行。此时的“三取二”降级为“二取二”。即只有在主、备机的运算结果一致时，方可对控制对象发送控制命令；否则，主、备机均不能对该控制对象输出(假设没有输出是可靠的，反之亦然，以下同)，一直等待，直到下述情况之一出现，方可继续对该控制对象发布控制命令：

·对该控制对象的运算结果主机和备机一致时；

·表决机恢复正常；

·主机和备机中的某一个出现硬件故障时：如主机发生硬件故障，则系统自动把备机变成主机；如果备机发生硬件故障，则由主机进行输出；

·人工干预。将故障主机或备机脱离该系统，不参与表决运算，同时报警。若故障机为主机，先将备机换成主机；若故障机为备机，则备机不再参与表决输出。短时间内由现役主机单机运行；在硬件故障修复后，由人工确认进入系统进行表决输出。

②一台执行机和表决机双机正常运行(另一台执行机故障)：这时“三取二”降级为“二取二”，即只有在执行机和表决机的运算结果一致时，方可对控制对象发送控制命令。若执行机和表决机的运算结果不一致，且两台机器都没有硬件故障，则执行机不能对控制对象输出。一直等待，直到下述情况之一出现方可继续对该控制对象发出控制命令：

·对该控制对象的运算结果主机和表决机一致时；

·另一台执行机恢复正常；

·主机和表决机中之一出现硬件故障时：若主机发生硬件故障，则系统停止输出并报警，此时该系统彻底不可用；若表决机发生硬件故障，则由主机进行输出，表决机脱离该系统，不再参与表决运算；

·人工干预，将备机脱离系统，不参与表决运算。若主机出现硬故障，则该系统停止工作，并报警；如果表决机出现硬件故障，则表决机自动脱离系统，同时报警，短时间内单机运行；在硬件故障修复后，由人工确认进入系统进行表决输出。

③ 主、备机均硬件故障时，系统停止工作，没有任何输出。

(3) 主机、备机和表决机三机运行(两台执行机和表决机正常工作)：

① 如果主机硬件故障，备机自动(或手工)成为主机，原主机脱离该系统，停止参与“三取二”运算，系统成为双机系统，即为(2)中的②所述。

② 备机硬件故障，原主机仍为主机正常工作，备机脱离系统，停止参与“三取二”运算，并报警，系统成为双机系统，即(2)中的②所述。

③ 表决机硬件故障，原主机仍为主机正常工作，表决机脱离系统，并报警，系统成为双机系统，即(2)中①所述。

④ 主机的输出结果和备机与表决机的输出结果不一致，此时，主、备机互换位置，按表决机结果进行输出。

⑤ 备机与主机和表决机输出结果不一致，主机不变，按表决机结果进行输出。

⑥ 表决机与主、备机输出结果不一致，主机不变，按主机结果进行输出。

3. **并行输出机制**

把图 1 中的采集和控制部分稍加改动，即成为并行输出机制模型。如图 2：

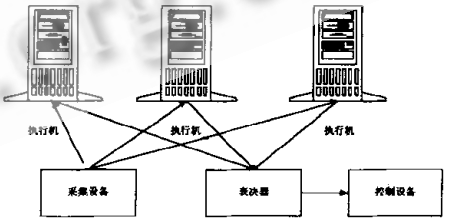

图 2　实时采集控制系统示意

图 2 为在并行输出机制中由三台执行相同功能的执行机和一个表决器组成的一个表决系统。在该系统中，和前面的主机输出机制一样，也是按照“三取二”的方式进行工作，只要三个执行机中的任何两个的输出结果一致，就认为这两个执行机没有故障，输出其结果。表决器的作用是选择三个执行机中至少两个一致的结果进行输出。但这种机制最大的弱点就是对表决器的依赖性太

强，如果表决器出现硬件故障，整个系统将陷入瘫痪，所以在可用性方面太脆弱。

4. 结论

从以上两种硬件冗余的分析，主机输出机制和并行输出机制在硬件方面的开销差不多，但它们的可靠性和可用性则有较大区别：

(1)故障检测和诊断方面：主机输出机制能够发现三台机器中任何一台或两台机器故障，并且报警；在有一台主机是完好的情况下，还可以进行正常工作。虽然这种机制并没有提高系统的可靠性，但它为及时处理故障提供了帮助。而并行输出机制则不能发现故障。

(2)可靠性方面：在主机输出机制中，只有一台执行机正常工作的情况下，该系统还可正常工作。而并行输出机制，至少要有两台主机正常工作的前提下，该系统才能正常工作。即并行输出机制的可靠性要高于主机输出机制。

(3)可用性方面：在主机输出机制中，只要有一台执行机正常工作，该系统仍可继续工作；若想进一步提高系统的可用性，可把表决机也设成具有输出功能。而在并行输出机制中，只有一台主机的情况下，该系统将停止工作。另外，由于并行输出机制采用了表决器，若表决器出现故障，则该系统将停止工作；而在主机输出机制中，无论哪台执行机作为主机，都可独立地进行输出控制。由此可见，主机输出机制的可用性要强于并行输出机制。

(4)故障切换和隔离方面：当发生故障时，主机输出机制系统具有故障检测和切换功能。当系统的某部分发生故障时，主机输出机制系统内部将故障机从系统中自动脱离，并根据具体情况判断是否倒换主机，使系统仍能保持正常工作。而在并行输出机制中，如果其中的一台发生硬件故障或软件模块出现问题，没有和其他两台同步，此时系统不能把故障机从系统隔离开，有可能使该故障主机的运算结果参与"三取二"表决运算，从而造成错误输出。

(来稿时间：1998 年 8 月)