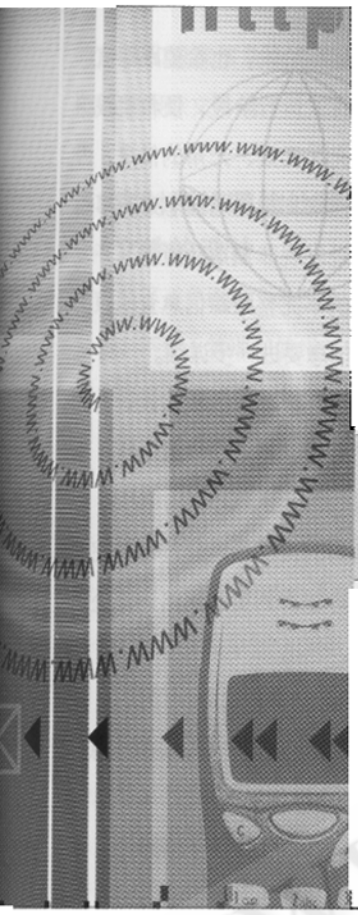

实时网络通信处理系统跟踪与审计设计

The Design of Real-time Network Communication Transaction System Tracing and Auditing

杨富玉 （北京中国金融电子化公司 100054）
单 纯 （北京理工大学软件学院 100081）

摘 要： 本文在分析实时网络通信处理系统的处理流程后，将实时网络通信处理系统的故障分类为预期故障和非预期故障。将实时网络通信处理系统的跟踪分类为完整级，基本级，最小级和不跟踪四个级别，并给出了相应的跟踪流程。同时设计了跟踪文件的格式。通过审计跟踪文件，可以监督系统的运行情况，改进系统设计，并对系统维护提供帮助。

关键词： 实时网络通信处理系统 中间件 故障 跟踪 审计

1 前言

随着计算机技术和网路技术的发展，越来越多的交易采用在计算机网络上用软件实现。尤其是在银行领域，网络化的计算机软件系统得到了广泛地应用。如正在全国逐步推广实施的中国现代化支付系统，将中央银行会计核算系统、国家金库会计核算系统、商业银行汇兑等连接起来，实现全国同城和异地资金的网上快速清算。与中国现代化支付系统相连的系统便存在相应的发送和接收网络通信程序，发送网络通信程序循环搜索业务数据库，将需要发送的数据进行处理，然后通过IBM CICS中间件发送给对方，接收网络通信程序通过IBM CICS中间件接收到对方发来的数据后进行处理，然后存入业务数据库。

发送和接收网络通信程序是不用人工干预的自动处理系统，由于网络软件运行的操作系统、网络通信状况非常复杂，需要发送的数据和接收到数据情况各异，通信软件的设计缺陷，中间件自身缺陷，通信软件开发漏洞等，都可能导致发送和接收网络通信程序不能正常地处理。windows server、linux操作系统和IBM CICS中间件自身存在性能跟踪机制，通过审计它们，可以对故障定位提供一些帮助。但无法替代对实时网络通信处理系统的内部跟踪。实时网络通信处理系统的内部跟踪，一方面可以作为通信日志，用作业务审计；另一方面通过审计跟踪文件，检查失效或者错误发生的条件、状态、后果，帮助开发者改正通信软件和改正业务处理系统，并可以帮助运行维护单位定位错误，正确地维护业务数据。如果实时网络通信处理系统没有跟踪审计处理或者跟踪审计处理设计的不妥当，便会给开发者错误定位和运行单位的运行维护带来很大困难。

2 实时网络通信处理系统与业务处理系统的关系

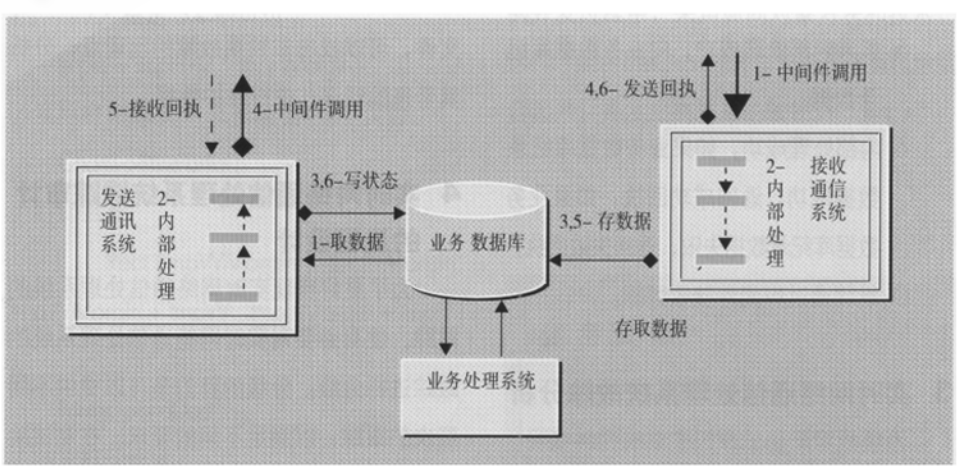

图 1 实时网络通信处理系统与业务处理系统的相互关系

图1表示实时网络通信处理系统与业务处理系统的相互关系。发送通信系统和接收通信系统处理流程如下。

发送通信系统处理流程：

0- 开始搜索业务数据库；

1- 发现业务数据库中存在需要发送的数据，从业务数据库中取数据；

2- 发送通信系统对取道的业务数据进行内部处理；

3- 如果2内部处理不成功，向业务数据库写状态；

4- 如果2内部处理成功，便将内部处理完成的内部数据调用中间件，完成网络发送；

5- 通过中间件接收对方的网络接收回执；

6- 根据回执情况，向业务数据库写状态；

0- 继续搜索业务数据库。

接收通信系统处理流程：

0- 开始准备通过中间件进行网络接收；

1- 通过中间件接收对方的传送数据；

2- 对接收到的数据，进行接收通信系统的内部处理；

3- 如果内部处理不成功,向业务数据库纪录内部处理失败日志；

4- 将处理失败的回执信息，调用中间件返回；

5- 如果内部处理成功，向业务数据库纪录数据；

6- 内部处理成功，如果业务数据库纪录数据成功，返回成功回执，如果业务数据库纪录数据失败，返回失败回执；

0- 继续通过中间件接收数据。

3 实时网络通信处理系统故障分析

系统故障产生的原因主要有两种情况：一种情况是由于系统内部错误，这主要是开发错误，包括需求理解不完整、设计缺限、编码错误等；另外一种情况是由于系统外部环境导致。无论何种原因导致的故障，我们都可以将实时网络通信处理系统的故障分为预期故障和非预期故障。

预期故障定义为在实时网络通信处理系统的处理流程中已经考虑到并存在相应的故障处理预案的故障。如接收通信系统的第6步，内部处理成功后，向业务数据库纪录数据发生故障。

非预期故障定义为实时网络通信处理系统的处理流程设计没有充分考虑，也不存在相应的故障处理预案的故障。如发送通信系统中的第6步，如果中间件调用发送回执成功，向业务数据库写状态出现失败。

预期故障和非预期故障是相对的，如果实时网络通信处理系统流程设计的好，并且开发的质量高，那么非预期故障便会较少，否则非预期故障便会较多。非预期故障出现的概率大少可以作为衡量实时网络通信处理系统设计开发好坏的标准之一。降低非预期故障出现的概率是可以做到，但是追求绝对不出现是不现实的。如由于操作系统发生意外，或者突然掉电导致实时网络通信处理系统处理异常而出现的故障，便很难避免。

基于非预期故障出现的必然性，设计实时网络通信处理系统的跟踪便显得非常必要和重要。开发者通过审查跟踪文件，可以发现非预期故障出现的条件，将非预期故障转化为预期故障。运行维护单位通过审查跟踪文件，可以找出非预期故障的出现点，分析其带来的错误，进行维护数据。

4 实时网络通信处理系统跟踪审计的流程设计

为了更好实现实时网络通信处理系统的跟踪，便有必要对实时网络通信处理系统的跟踪进行分级。分级的目的是可以提供不同层次的跟踪，以满足不同的要求。在测试阶段，开发者希望尽可能多的跟踪信息，以帮助开发者检查程序的运行流程是否满足设计开发要求。在试运行阶段，也希望跟踪信息尽可能完整。在正式运行阶段，便希望跟踪信息有效，不要充斥无效、无用的信息，否则运行维护单位无法利用跟踪信息进行事后监督。但是在已经发现非预期故障后，开发者无法利用已有的不完整跟踪信息查明原因时，便希望跟踪信息要进一步详细。

实时网络通信处理系统的跟踪设计为如下四个级别：完整级；基本级；最小级；不跟踪，并分别用1、2、3、0代表。

完整级要达到的目标是，通过审查完整级的跟踪文件，可以得到实时网络通信处理系统的数据流程，包括：

（1）程序的启动停止信息；

（2）所有的循环开始，进行，结束信息；

（3）对数据库操作的信息；

（4）对数据进行处理前的数据状态，处理过程，处理后的数据状态；.

（5）将所有的函数级操作信息都要进行跟踪纪录；

基本级要达到的目标是，通过审查基本级的跟踪文件，可以得到实时网络通信处理系统的程序流程，包括：

（1）程序的启动停止信息；

（2）所有的循环开始，结束信息；

（3）对数据库的写操作信息；

（4）对基本函数进行数据处理前的数据状态和处理后的数据库状态；

最小级要达到的目标是，通过审查基本级的跟踪文件，可以得到实时网络通信处理系统的业务流程，程序出现错误的地方及状态，包括：

（1）业务流程的开始信息和结束信息；

（2）所有函数的错误返回信息。

不跟踪的设置，便是将跟踪功能关闭。

有了分级设计后，实时网络通信处理系统处理的跟踪流程如下：

（1）实时网络通信处理系统启动时获取配置文件中的跟踪级别；

（2）根据跟踪级别纪录跟踪信息（跟踪

文件名和跟踪信息格式请见实时网络通信处理系统跟踪文件的设计）。

5 实时网络通信处理系统跟踪审计文件的设计

为了避免跟踪文件过大，导致写文件效率降低，不便于管理和使用，将跟踪文件设置为一个帐务日期或者机器日期一个跟踪文件。

跟踪文件内容格式：

机器时间；跟踪类别；业务流程名称；程序流程名称（或父函数名称）；函数名称；函数位置；处理前状态；处理后状态；备注(包含错误原因，如数据库返回错误原因，网络错误原因等)。

例如：跟踪文件20030401.log，其中一条跟踪信息如下：

20030401 11：08：01；3；发送汇兑资金；回执处理；f_write_statustodb；12行；nameno='001',status='1'；失败；update表sending失败，没有找到nameno='001'的纪录。

这条跟踪信息说明，在2003年4月1日11时8分1秒，通过最小级跟踪方式发现，发送汇兑资金业务流程中，在回执处理阶段，函数f_write_statustodb中12行，对sending表更新nameno等于001的status信息为1时失败，原因是：sending表不存在nameno等于001的纪录。

6 结论

就像飞行记录仪的作用一样，通过分析飞行记录仪的纪录，可以对飞行过程进行监督，如果出现意外，通过分析飞行记录仪的纪录，可以推测出故障产生的原因。对于实时网络通信处理系统，由于有了强有利的跟踪措施，通过审计跟踪文件，进行定期的监督。对待其中暴露出的问题，通过对跟踪文件的分析，了解故障发生前的系统运行情况，作为判断故障原因的依据，及时采取相应对策，保证实时网络通信处理系统地正常运行，并对系统的改进提供帮助。

参考文献

1 Microsoft Corp, Event Tracing for Windows (ETW) [EB/OL], http: //msdn.microsoft.com / library /en-us/ perfmon/base/ event_tracing.asp, 2002。

2 K. Yaghmour and M. R. Dagenais. Measuring and characterizing system behavior using kernel-level event logging[R]. Proc.USENIX Annual Technical Conference, June 2000。

3 Shari Lawrence Pfleeger.SOFTWARE ENGINEERING Theroy and Practice[M].北京:高等教育出版社，2001.1-20。

4 杨孝如等，SYBASE 数据库系统管理指南[M]，中国水利水电出版社，1997.10-40。