文章编号:1671-4598(2023)06-0087-07 DOI:10.16526/j.cnki.11—4762/tp.2023.06.014 中图分类号:TP311.56 文献标识码:A

测发控系统前置测控软件热备冗余研究

谢 望,兰旭东,高 飞,赵新航,卫吉祥,徐 昕
(上海航天电子技术研究所,上海 201109)

摘要:前置测控软件是运载火箭地面测发控系统中的重要组成部分,主要负责试验和发射中运载火箭的地面部分数据的采集和显示以及控制,具有实时性强、可靠性高、数据量大和接口关系复杂等特性;针对目前航天发射呈现任务高密度常态化,试验次数增多,对前置测控软件的可靠性需求提高的问题,研究了基于心跳信号的热备冗余系统,通过设置主备两份软件以及互相之间心跳信号通信的方式,在主份软件故障情况下,可实现软件冗余系统自主切换,提升了在试验过程中前置测控软件和地面测发控软件系统的整体可靠性,保证了软件在运载火箭在测试和发射试验中的稳定性,为未来运载火箭地面测发控系统软件可靠性研究提供了思路;

关键词:地面测发控;前置测控软件;热备冗余;心跳信号;可靠性研究

Research on the Hot Standby Redundancy of the Pretest and Control Software of the Test and Control System

XIE Wang, LAN Xudong, GAO Fei, ZHAO Xinhang, WEI Jixiang, XU Xin
(Shanghai Institute of Aerospace Electronics Technology, Shanghai 201109, China)

Abstract: The pretest and control software is an important part of the ground test and control system of the carrier rocket. It is mainly responsible for the acquisition, display and control of the ground data of the carrier rocket during test and launch. It has the characteristics of strong real-time performance, high reliability, large data and complex interface relationship. Aiming at the problems of mission density normalizing in space launch, increasing test times, and increasing reliability requirements of the pretest and control software, a hot standby redundancy system based on heartbeat signals is studied. By setting the primary and secondary software and communicating with each other through heartbeat signals, the autonomous switching of the software redundancy system can be realized in case of the failure of the primary software, which improves the overall reliability of the pretest and control software system and ground test and development control software system in the test process , ensures the stability of the software in the test and launch test of the carrier rocke, and provides a idea for the reliability research of the ground test and development and control system software of the carrier rocket in the future.

Keywords: ground test and control; pre-test and control software; hot standby redundancy; heartbeat signal; reliability study

0 引言

地面测发控系统是运载火箭地面系统的重要组成部分,负责完成运载火箭的集成综合测试和发射试验[1-5]。而在运载火箭地面测发控系统中,软件是重要的一环。软件质量和软件的可靠性是软件生存的基本条件[6-7],也是软件人员追求的目标,提高软件质量是软件开发过程中的关键问题[8]。提高软件质量和可靠性通常有两种方法:避开错误和容错。任何软件都不能做到没有错误,因此完全避开错误是不可能的,容错技术可以使错误发生时系统不受影响或受到的损害最小,冗余技术是容错方法中的主要技术[9-11]。

为了避免某个部件故障给系统工作带来影响,通常采用部件的备份冗余设计方案,在多软件协同工作系统中,任何一个软件发生故障,都与可能导致整个软件系统无法正常工作,而通常软件也可以进行备份冗余设计。在多软件组成的软件系统中,可以对某个软件进行备份,如果这个软件发生故障,则可以立即启动备份计算机上的备份软件继续工作,达到不影响整体软件系统运行的效果[12-13]。

目前航天八院运载地面测发控系统领域,还未开展核心软件热备冗余自主切换设计,地面核心软件运行故障会直接导致试验停滞,影响试验进度及测试效率。随着航天事业的迅猛发展,航天发射任务日益繁重,呈现任务高密度常态化、任务并行多和技术状态新等新特点,对地面核心软件系统的可靠性提出了更高要求,如何解决核心关键软件可靠性问题是本论文研究的重点。

在运载火箭试验中,地面测发控系统的前置测控软件具有实时性强、可靠性高、数据量大和接口关系复杂等特性,主要完成测量数据实时采集、实时数据处理、状态显示和通道控制等任务,其重要性不言而喻。前置测控软件的可靠运行,对实现实时测量与控制至关重要,如果前置

收稿日期:2023-03-06; **修回日期**:2023-03-13。
作者简介:谢 望(1996-),男,安徽安庆人,硕士,助理工程师,主要从事运载火箭地面测发控系统软件技术方向的研究。
引用格式:谢 望,兰旭东,高 飞,等.测发控系统前置测控软件热备冗余研究[J].计算机测量与控制,2023,31(6):87-93,100.

测控软件发生故障，则会直接导致试验的停止。

在上述背景下，本论文从提升核心软件可靠性方向出发，研究在线热备冗余切换技术，在软件一度故障情况下，可实现软件冗余系统自主切换，提升软件系统整体可靠性，降低个别软件运行故障对试验整体进程的影响，取消依托人工更换备份设备的模式。

1 热备冗余系统软件设计原理

1.1 数据链路和软件模块

本论文设计的软件冗余为主备双软件冗余，前置测控软件分为主前置测控软件和备前置测控软件两份，在正常工作状态下，主前置测控软件保持在工作状态，备前置测控软件保持在待机状态。若主前置测控软件发生故障，热备冗余系统可以及时发现故障并进行处理，备前置测控软件在要求的时间内，可以从待机状态切换为工作状态，继续接替原来的主前置测控软件进行工作。

在进行数据链路的设计之前，需要将主前置测控软件和主备前置测控软件以及地面测发控软件系统之间的信息流进行梳理：如图 1 所示，在没有故障发生的正常状态下，一条控制指令的执行会产生 5 条数据流，下面按照图中的编号顺序进行说明，数据流①是从主机控制软件发送到服务器软件的控制指令的数据流，主机控制软件每发送一条控制指令，就会出现一条数据流①，当数据流①到达服务器软件之后，服务器软件会对数据流①进行解析，重点关注的是数据流①中包含的信宿信息，信宿信息代表了此条指令最终需要到达的目的地。在主备前置测控软件均开启之后，它们都会主动和服务器软件进行网络连接。服务器软件会将主备前置测控软件的信宿设置为相同，那么服务器软件在解析数据流①之后，会给主前置测控软件和备前置测控均进行转发数据，也就产生了数据流②和数据流③，这两份数据流中的信息完全相同，均从服务器软件发出，到达主前置测控软件和备前置测控软件。主前置测控软件在收到数据流②之后，主前置测控软件根据自身的“主”状态，进行数据流②的解析，解析之后获取数据流②中包含的控制指令，然后根据控制指令对下游硬件板卡进行相应的控制，控制指令执行结束之后，主前置测控软件会在软件页面上进行控制指令的流程显示，这样试验人员就可以清楚地知道控制指令的执行进度。除了进行控制指令的显示之外，主前置测控软件还要将指令执行结果进行回令，因此主前置测控软件会进行数据流④的发送。数据流④到达服务器软件之后，服务器软件会解析数据流④中包含的信宿信息，主前置测控软件在组织数据流④的时候，会在信宿信息中填入主机控制软件的信宿编号，因此服务器软件就会将数据流④转发给主机控制软件，因此也就有了数据流⑤，也就是从服务器软件到主机控制软件的控制回令。主机控制软件在收到数据流⑤之后，进行数据流⑤的解析，在确认控制回令的正确性之后，这条控制指令的执行才算正式结束。需要注意的是，备前置测控软件在收到数据流③之后，备前置测控软件根据自身的“备”状态，也会进行数据流③的解析，解析之后获取数据流③中包含的控制指令，但是它并不会对下游硬件板卡进行控制，并且备前置测控软件也不会发送回令数据流。从图 1 也可以发现，从服务器软件到备前置测控软件的信息流是单向的。解析完数据流②之后，备前置测控软件会在页面上进行控制指令的流程显示，这样试验人员也可以清楚的在备前置测控软件的页面上获取当前控制指令的执行进度。

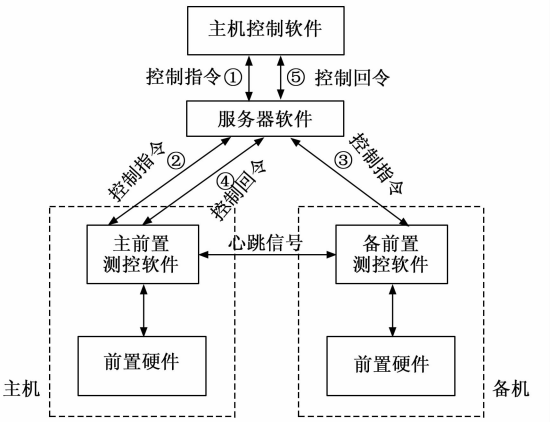

图 1 热备冗余系统数据链路图

在设计了双软件冗余之后，自动控制组合之间需要进行状态同步、故障监测和状态切换，因此主前置测控软件和备前置测控软件之间也需要进行网络通信。主前置测控软件和备前置测控软件之间，除了需要随时知道彼此的故障与否，还需要知道对方目前的工作状态，以便进行主备软件切换判断和工作流程进度上的接续。因此，主前置测控软件和备前置测控软件之间，设计了从主前置测控软件到备前置测控软件的实时“心跳”信号，根据“心跳”信号，备前置测控软件就

能实时地获取到主前置测控软件的状态和是否出现故障信息。主前置测控软件和备前置测控软件之间，除了“心跳”信号之外，有时候还需要进行其他信息的交换，所以主前置测控软件和备前置测控软件之间也是需要设计通信数据链路。因此，就形成了主机控制软件、主前置测控软件和备前置测控软件三者之间的数据链路。

在设计完热备冗余系统数据链路之后，前置测控软件就需要增加之前没有的模块，除了它本身的初始化 PXI 板卡、接受并解析控制指令和执行控制指令之外，为了实现热备冗余系统，需要增加“心跳”信号发送模块、“心跳”信号解析模块、主备切换模块和时串计数发送模块。因此此处介绍一下前置测控软件的模块划分，如图 2 所示：前置测控软件的核心功能是下游 PXI 硬件板卡的控制和数据监测，图中的控制指令接收模块、控制指令解析模块和控制指令执行模块用于 PXI 硬件板卡的控制，PXI 板卡初始化模块用于对 PXI 硬件板卡的初始化工作，工作过程中 PXI 硬件板卡的数据会上传到前置测控软件内部的监测模块，实现对 PXI 硬件板卡的数据实时监测。新增的用于热备冗余系统的模块包括：软件初始化模块、主备状态切换

模块、“心跳”信号发送接收模块和时串计数接收发送模块，软件初始化模块除了进行软件和硬件的初始化之外，还用于热备冗余系统的热备冗余机制启动。主备状态切换模块，接收“心跳”信号接收模块传递过来的“心跳”信号和时串计数接收模块发送过来的时串计数信号，根据“心跳”信号决定前置测控软件的主备状态和后续的跳变动作执行。上述几个模块就是前置测控软件的主体部分，使得前置测控软件具备了测控和主备切换的功能。

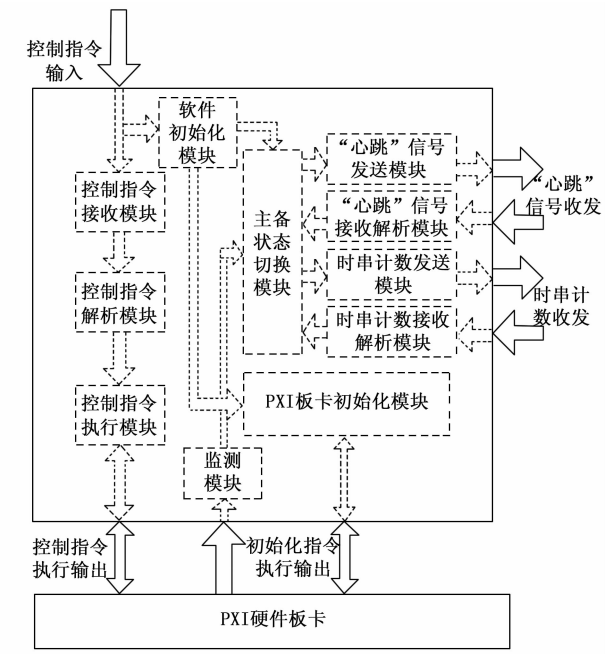

图 2　前置测控软件内部模块示意图

1.2　“心跳”系统设计

在 1.1 中已经说明，主备前置测控软件之间同样也需要进行通信，其目的是为了让互相冗余的软件知道彼此的状态，进而决定自己的工作状态和后续动作。设计的系统中，将主备前置测控软件之间的通信信号称为“心跳”信号。在正常工作情况下，主前置测控软件通过 UDP 单播方式向备前置测控软件发送“心跳”信号，备前置测控软件接收主前置测控软件发来的“心跳”信号并进行解析，通过“心跳”信号获取对方的工作状态。当备前置测控软件切换成主前置测控软件之后也需要对外发送“心跳”信号，因此主备前置测控软件都要能够具备发送“心跳”信号和接收解析对方发来的“心跳”信号的功能。

在设计的软件热备冗余系统中，在正常状态下，主前置测控软件正常工作，除了进行工作操作之外，还向备前置测控软件发出正常的“心跳”信号，备前置测控软件在正常状态下，接收到主前置测控软件发来的“心跳”信号。如果主前置测控软件下游的硬件发生了故障，主前置测控软件监测并发现了故障，此时主前置软件本身没有出现故障，依然能对外发送“心跳”信号，但此时需要改变发送的“心跳”信号的内容，改为发送异常“心跳”信号。而对于备前置测控软件来说，不管是正常的“心跳”信号还是异常的“心跳”信号，都需要进行接收和解析。

下面进行“心跳”信号的内容和判别算法的说明，设计的“心跳”信号数据帧为 10 个字节，数据帧的内容如表 1 所示。

表 1　心跳信号数据帧内容

内容	帧头	数据帧发送时间	心跳内容	校验和	帧尾
字节长度	2	4	2	2	1

帧头采用运载火箭地面测发控系统的帧头，第一个字节为 0XEB，第二个字节为 0x90，作为一个数据帧的开始，数据帧发送时间一共 4 个字节，填充这个数据帧的发送时间，心跳内容一共分为 2 种，在正常情况下，“心跳”信号中的心跳内容字节填充的是 0x00，异常情况下“心跳”信号中填充的心跳内容为 0x55。检验和占据 2 个字节，将整个数据帧除去这 2 个字节的其他 8 个字节进行累和之后按位取反再加 1，将计算结果填入这 2 个字节之中，帧尾为 1 个字节，填入 0xDD，表明这个数据帧的结束。在设计的主前置测控软件中，以 200 ms 一帧的速率定时向备前置测控软件发送“心跳”信号数据帧，备前置测控软件进行“心跳”信号的接收和解析，而关于心跳信号的判别算法，在 1.3 中进行详细描述。

1.3　热备冗余系统设计

图 3 和图 4 分别是设计的主前置测控软和备前置测控软件工作流程图。切换系统是根据“心跳”信号进行工作的。对于主前置测控软件来说，在工作的过程中需要对软件下游硬件是否进行故障进行判断，如果没有出现故障，则发送正常的“心跳”信号给备前置测控软件，并正常执行工作流程，对主机控制软件发来的控制指令进行解析，对软件下游硬件下达执行指令，实时显示执行的流程进度，同时按照主机控制软件的要求给主机控制软件进行每一条指令的回令。如果监测中发现了软件下游的硬件故障，则主前置测控软件立即给备前置测控软件发送异常的“心跳”信号。

对于备前置测控软件来说，在没有切换成主前置测控软件之前，同样会收到主机控制软件的指令信息，不同于主前置测控软件，备前置测控软件在收到控制指令并解析之后并不会对下游硬件下达执行指令，也不会对主机控制软件进行回令，只是实时显示收到的流程进度，保证了系统中的三个软件均能对外显示系统中的工作执行进度。

备前置测控软件会实时接收主前置测控软件发来的“心跳”信号并进行检测，因为主前置测控软件发生故障之后，会发送出异常的“心跳”信号给备前置测控软件，备前置测控软件在解析“心跳”信号数据帧的时候，解析出来的心跳内容如果为 0x00，则表明这帧“心跳”信号为正常的心跳信号，如果解析出来的数据帧中的心跳内容为 0x55，则可以判定这帧“心跳”信号为异常“心跳”信号。此时备前置测控软件就会进行主备状态的切换，在切换完成之后，由备前置测控软件代替原来的主前置测控软件参

与工作，此时对接受到的主机控制软件发送来的指令进行解析，并对下游硬件发送控制指令，同时给主机控制软件发送回令，并且继续显示执行的流程进度，这样就保证了工作流程进度的持续和完整。除此之外，切换之后的软件也会和故障前的主前置测控软件一样，对外发送“心跳”信号，表明本软件已经切换为主软件状态，如果此时有新的前置测控软件增加到系统中来，也会收到“心跳”信号，就可以获取到此时系统中的主前置测控软件的存在信息。

如果主前置测控软件发生运行异常退出、宕机，或者是主前置测控软件发生网络异常，无法连接上局域网，无法对外发送网络信号，都会影响到“心跳”信号的发送，则此时备前置测控软件就无法接收到“心跳”信号，对于备前置测控软件来说也就是“心跳”信号暂停，备前置测控软件设计的解析“心跳”信号模块中，会首先解析“心跳”信号的心跳内容，如果心跳内容为 0x00，则表明这个心跳信号目前为正常的心跳信号，再进行下面的“心跳”信号中包含的时间信息的解析，将“心跳”信号中的 4 个字节表示的信息帧的发送时间解析出来，并和当前的备前置测控软件这台计算机上的系统时间进行比对，如果时间误差在 20 ms 以为，则认为此时的“心跳”信号的时间正常，如果没有收到“心跳”信号，则随着备前置测控软件所在的计算机上的系统时间的更新，则计算出来的时长也就会逐渐变大，然后对时长进行判断，设定的时长阈值为 5 秒，在超出时间阈值之后，备前置测控软件就可以判定主前置测控软件发生了运行异常退出、宕机，或者是网络异常，此时备前置测控软件就进行切换成主前置测控软件进行后续工作。设计的时长阈值进行了可配置设置，针对不同的系统，可以灵活设置不同的时长阈值，保证了不同系统都能在有效并且合适的时间内完成切换。

在工作人员发现故障并进行故障的排除之后，重新启动软件，此时系统中已经存在主前置测控软件并以相同的速率对外发送“心跳”信号，在接收到“心跳”信号之后，重新启动的软件自动设置自身模式为备份状态，成为此时系统中的备前置测控软件，对此时系统中正在工作的主前置测控软件进行冗余备份，和之前的备前置测控软件完全一样，在收到控制指令并解析之后并不会对下游硬件下达执行指令，也不会对主机控制软件进行回令，只是实时显示收到的流程进度。图 3 和图 4 是主前置测控软件和备前置测控软件的工作流程图。

在实际进入工作状态之前，需要将整个热备冗余系统进行启动，并进行初始化。在初始化阶段，不论是主前置测控软件还是备前置测控软件，初始化的时间点，初始化所需要的时长均不固定，此时在初始化之前，热备冗余系统容易产生误判，如果工作人员首先开启备前置测控软件，备前置测控软件在开启之后的一段时间内均没有开启主前置测控软件，那么按照热备冗余系统的设计，在 5 秒钟没有接收到“心跳”信号之后，备前置测控软件就会自动的切换自身的状态变为主前置测控软件，如果此时工作人员

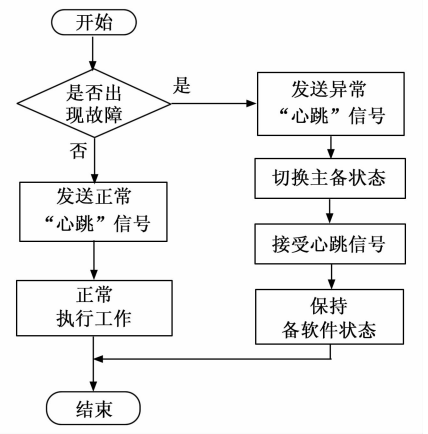

图 3 主前置测控软件工作流程图

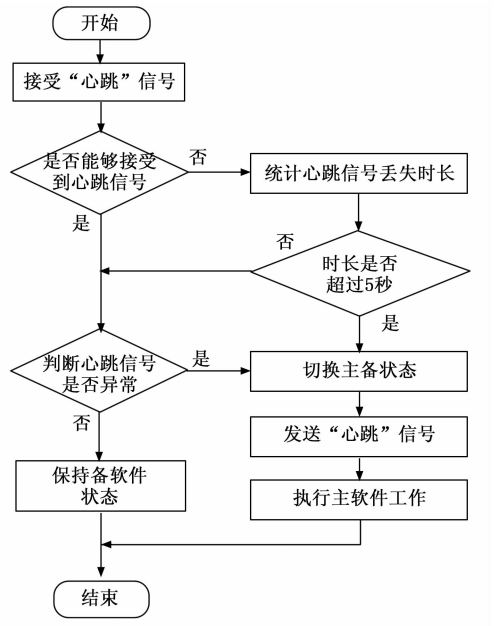

图 4 备前置测控软件工作流程图

继续开启主前置测控软件，主前置测控软件初始化之后监测到自己收到了“心跳”信号，则会将自身的状态切换成备份状态，这种跳变就属于是无效跳变，不仅会浪费时间并且可能会对试验进程造成影响。为了让设计的热备冗余系统的跳变更加的灵活和实用，将主备热备冗余软件设计成在初始化之后的检测和跳变设置为非使能状态，换言之在主备前置测控软件初始化的时候，不进行故障状态的监测和切换，而在主机控制软件中添加一条热备冗余机制开启指令，只有在工作人员将这条指令发送给初始化完成好的主备前置测控软件之后，主备前置测控软件在收到这条控制指令之后，才会开启故障监测和心跳模块，让热备冗余切换变得更加的有规律和稳定，消除了初始化过程中容易出现的问题。

下面对设计的热备冗余系统的初始化进行描述，首先开启服务器软件，然后开启主机控制软件并和服务器软件进行网络连接，然后开启主前置测控组合的计算机，开启

主前置测控软件，等待初始化 PXI 板卡完毕，然后主前置测控软件连接服务器软件，连接完成之后再开启备前置测控组合的计算机，开启备前置测控软件，同样等待初始化 PXI 板卡完毕，再和服务器软件进行网络连接，网络连接都完成之后，从主机控制软件上向主备前置测控软件发送热备冗余机制开启指令，将主备前置测控软件的热备冗余机制开启，至此主备前置监测组合的初始化工作才算完成。

2　故障情况分析及应对

在实际的前置测控软件热备冗余系统中，结合运载火箭地面测发控系统日常工作，从硬件和软件层面，总结出如下 6 种故障模式，列举在表 2 中。

表 2　故障类型说明

故障类型编号	故障模块	故障详细情况
1	前置测控软件	前置测控软件异常退出或者宕机
2	网络通信	前置测控组合网卡故障
3	网络通信	前置测控组合通信网线物理损坏
4	PXI 硬件	PXI 硬件板卡检测到数据边界值溢出
5	PXI 硬件	PXI 硬件板卡控制接口返回值不正确
6	PXI 硬件	PXI 硬件板卡初始化失败

在梳理了这几种故障类型之后，在实验室进行这几种故障类型的模拟，用于检测设计的热备冗余系统是否可以监测到故障并完成热备冗余的切换。故障的模拟的试验在实验室手动进行，考虑到前置测控软件的实际工作状态，将模拟试验的前置条件均设置为如下两种情况：第一种是主机控制软件还没有给主前置测控软件发控制指令，指令执行流程并没有开始，第二种是主机控制软件已经开始给主前置测控软件发送控制指令了，在某条指令的执行流程完全结束之后进行故障类型的模拟。

1）前置测控软件异常退出和前置测控软件异常宕机：这两种故障情况是考虑到软件本身层面和硬件层面，因为运载火箭试验时间久，指令多，在上位机上长时间运行的前置测控软件可能会出现异常崩溃退出，或者出现异常宕机的情况。在实验室进行这种故障类型的模拟，分为如下几种情况，第一种是将主前置测控软件所在的计算机进行突然掉电处理，第二种是将主前置测控软件进程强制关闭，第三种是使用主前置测控软件提供的“主软件异常关闭”故障模拟按钮进行这种故障的模拟，这个按钮的底层实现逻辑也是将本软件的进程强制关闭。在实验室中进行两种前置条件下的三种不同故障方式的模拟。主前置测控软件在出现异常之后，备前置测控软件会在较短的时间内进行状态切换，从“备”状态切换为“主”状态，然后继续和其他系统软件一起准备进入工作状态或者是继续工作状态。这种故障能及时切换的原因如下：主前置测控软件出现了异常退出或者宕机的情况，影响到整个主前置测控软件的运行，那么此时主前置测控软件对外发送“心跳”信号的动作也就无法完成了，此时系统中从主前置测控软件发往备前置测控软件的“心跳”信号也会消失。待机状态的备前置测控软件在没收到“心跳”信号之后，进行时长统计，如果未收到的时长超过 5 秒钟，也就是说主前置测控软件出现了超过 5 秒钟的软件异常退出或者宕机，则可以判定为主前置测控软件发生了软件故障，就会进行后续主备状态切换处理。

2）前置测控组合网卡故障：这种故障情况是考虑到前置测控软件所在的上位机的网卡可能会在长时间工作的过程中出现硬件和驱动上的问题，通过在上位机上进行网卡适配器突然禁止使用的方法进行这种故障的模拟。在实验室中进行两种前置条件下的这种故障方式的模拟，试验的结果是主前置测控软件在出现异常之后，备前置测控软件会在较短的时间内进行状态切换，从“备”状态切换为“主”状态，然后继续和其他系统软件一起准备进入工作状态或者是继续工作状态。这种故障能及时切换的原因和 1）相同，在出现网卡故障之后，主前置测控软件同样无法对外发送“心跳”信号，那么备前置测控软件超过 5 秒钟没有收到心跳信号，则也可以判定为前置测控软件发生了网络故障，同样进行后续主备状态切换处理。

3）前置测控组合通信网线物理损坏：这种故障情况是考虑到在试验的过程中，使用的网线可能会出现老化故障，或者是外界物理因素导致网线物理损坏，失去网络通信功能。实验室中进行了两种不同的故障模拟方法，第一种是直接将主前置测控软件所在的上位机和地面测发控系统交换机之间的网线进行剪断，第二种是手动将主前置测控软件所在的计算机和测发控系统交换机之间的网线进行断开物理连接。在实验室中进行两种前置条件下的这两种故障方式的模拟，试验的结果是主前置测控软件在出现这种网络故障之后，备前置测控软件会在较短的时间内进行状态切换，从“备”状态切换为“主”状态，然后继续和其他系统软件一起准备进入工作状态或者是继续工作状态。这种故障能及时切换的原因也和 1）相同，在出现网线故障之后，主前置测控软件同样无法对外发送“心跳”信号，那么备前置测控软件超过 5 秒钟没有收到心跳信号，则也可以判定为主前置测控软件发生了网络故障，同样进行后续主备状态切换处理。

4）PXI 硬件板卡检测到数据边界值溢出：在试验的进行过程中，前置测控软件不仅仅是对 PXI 硬件板卡下达控制指令，还需要监测外界系统电缆传递过来的较多的数据信息，前置测控软件在设计的过程中需要提前将需要监测的各项数据的边界值进行预设，当数据到达 PXI 硬件板卡之后，前置测控软件的监测模块会对板卡采集到的数据进行判断，如果数据在预先设计的范围之内，那么认为这这个数据是正常的，如果收到的数据在预先设置的范围之外，此时无法确定是传递过来的数据异常还是 PXI 硬件板卡的采集出现问题，那么此时前置测控软件均可以认为是 PXI 硬件板卡出现故障，那么此时也应该进行主备软件的跳变切换。对于这种故障类型，实验室中进行的方法是将输入 PXI 机箱的某几项数据手动的设置超出最大值的数据值，

观察到主前置测控软件在监测到异常数据值之后，备前置测控软件在较短时间内从“备”状态切换为“主”状态，然后继续和其他系统软件一起准备进入工作状态或者是继续工作状态。这种故障能及时切换的原因是因为主前置测控软件在监测到异常的数据之后，判定是主前置 PXI 硬件板卡故障，然后立即对备前置测控软件发送异常的“心跳”信号，备前置测控软件在收到异常的“心跳”信号之后，可以认为主前置测控软件发生了网络故障，同样进行后续主备状态切换处理。

5）PXI 硬件板卡控制接口返回值不正确：在试验的进行过程中，前置测控软件需要对 PXI 硬件板卡下达控制指令，但是控制指令的执行可能成功也有可能失败，PXI 硬件板卡的驱动提供的底层执行函数上，通过函数的返回值来判断控制指令的执行成功与否，因此前置测控软件在调用 PXI 硬件板卡驱动提供的执行函数之后，需要对某些执行函数的返回值进行判断，如果执行的函数返回值表明函数执行失败，那么表明此时前置测控软件的这条控制指令就没有执行成功，此时前置测控软件就可以判定 PXI 硬件板卡出现了故障，那么此时也应该进行主备软件的跳变切换。对于这种故障类型，实验室中进行的方法是在代码中将 PXI 硬件板卡的驱动的底层执行函数的返回值进行手动取反之后再提供给前置测控软件的调用函数，这样前置测控软件的调用函数接收到的返回值就出现了异常，观察到主前置测控软件在监测到异常的 PXI 硬件板卡控制接口返回值之后，备前置测控软件在较短时间内从“备”状态切换为“主”状态，然后继续和其他系统软件一起准备进入工作状态或者是继续工作状态。这种故障能及时切换的原因是因为主前置测控软件在监测到异常的接口返回值之后，判定是主前置 PXI 硬件板卡故障，然后立即对备前置测控软件发送异常的“心跳”信号，备前置测控软件在收到异常的“心跳”信号之后，可以认为主前置测控软件发生了网络故障，同样进行后续主备状态切换处理。

6）PXI 硬件板卡初始化失败：在试验的开始阶段，前置测控软件需要进行 PXI 硬件板卡初始化，PXI 硬件板卡初始化工作完成之后，前置测控软件才能和 PXI 硬件板卡配合工作，但是初始化工作可能会出现某块板卡初始化失败的情况，因此在主前置测控软件的代码中对 PXI 硬件板卡初始化函数的返回值进行判断，如果返回值不正确或者 PXI 硬件板卡的初始化函数无法调用，则前置测控软件也可以认为出现了 PXI 硬件板卡故障，那么此时也应该进行主备软件的跳变切换。对于这种故障类型，实验室中进行的方法是将某块 PXI 硬件板卡的驱动进行单独卸载，然后正常启动前置测控软件去尝试初始化所有的 PXI 硬件板卡，出现的现象是软件在启动完毕后，卸载了驱动的 PXI 硬件板卡会出现初始化失败，后续备前置测控软件会在较短时间内从“备”状态切换为“主”状态，然后继续和主机控制软件，服务器软件一起准备进入工作状态或者是继续工作状态。这种故障能及时切换的原因是因为主前置测控软件在监测到 PXI 硬件板卡初始化失败之后，判定是主前置 PXI 硬件板卡故障，然后立即对备前置测控软件发送异常的“心跳”信号，备前置测控软件在收到异常的“心跳”信号之后，可以认为主前置 PXI 硬件板卡发生了故障，同样进行后续主备状态切换处理。

图 5 是对上文描述的 6 种故障的分类图示，根据故障模块将 6 种故障类型分为 3 大类，分别是前置测控软件故障、前置测控组合网卡或者网线故障和 PXI 硬件故障。其中前面两种故障大类包含故障类型 1）－3），这 3 种故障类型对系统中心跳信号的影响都是会使得心跳信号的消失，第三种故障大类包含故障类型 4）－6），这 3 种故障类型对系统中心跳信号的影响是使得心跳信号从正常信号变为异常信号，在实验室的故障模拟中热备冗余系统均能出现正确及时的故障监测并进行主备前置测控软件的跳变，保证系统的工作不受影响。

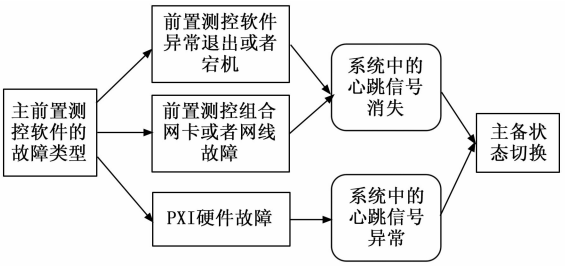

图 5 模拟故障类型列举

需要说明的是，本论文设计的热备冗余系统中的主备软件中的“主”和“备”不是固定的，而是互为主备，主备软件的代码设计完全相同，软件初次启动的时候通过读取配置文件的方式来确定主备状态，或者是通过主机控制软件来进行远程控制软件的主备状态。在主前置测控软件出现故障之后，主前置测控软件从系统中暂时脱离，此时备前置测控软件切换为主软件状态，而当工作人员将原来的主前置测控软件中的故障进行恢复之后，重新启动软件，此时启动的软件能够收到系统中的现存的主前置测控软件发来的“心跳”信号，即使此时读取的配置文件信息为主软件状态，但是设定“心跳”信号的优先级更高，因此重新启动的软件将保持为“备”状态。如果此时系统中正常工作的主前置测控软件再次出现故障，那么此时重新启动之后保持为备用状态的前置测控软件也可以切换为“主”状态进行工作，实现主备冗余的互相切换，保证了系统工作的稳定性。

3 时串发送系统设计

实际的前置测控软件，不仅需要接受主机控制软件的控制指令并回令，也会给主机控制软件发送时串，如果在发送时串的过程中出现故障，无论是软件异常退出或者宕机、前置测控软件出现网络中断和前置测控软件下游的硬件异常中的哪一种故障模式，主前置测控软件的时串发送过程都会中断。

为了发生故障之后不影响时串发送，备前置测控软件切换主备状态之后不仅仅需要继续给主机控制软件发送时串，并且要准确的知道时串的发送进度，需要从下一个还没有发送的时串处开始进行发送，不能出现某一条时串的重复发送，同样也不能出现时串的发送遗漏。因此在主前置测控软件给主机控制软件发送时串的同时，需要在“心跳”信号中添加已经发送的时串计数，而备前置测控软件在接受到“心跳”信号并检测的同时，需要将时串计数保存，每次收到“心跳”信号之后都会进行时串计数的更新，保证此时此刻软件中存储的时串计数都是最新的。如果在主前置测控软件在发送时串的过程中发生故障导致时串发送停止，那么在备前置测控软件切换成主状态之后，需要继续给主机控制软件发送时串，根据之前在“心跳”信号中保存下来的时串计数，此时的切换主备状态之后的前置测控软件就可以从时串序列计数的下一个时串处开始发送，能够保证时串的不中断不重复发送，保证时串发送工作的连续性和完整性。图 6 是主前置测控软件发送时串时发生异常导致发送中断之后的切换示意图。

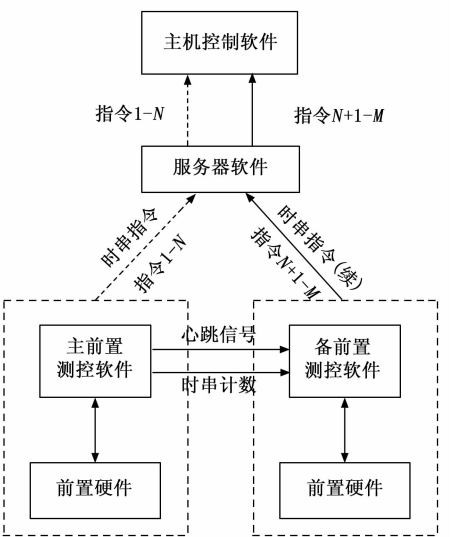

图 6　时串发送中止后切换示意图

4　主备切换时间验证

设计的热备冗余软件系统用于实际工作过程中，主备软件的切换时间需要进行严格要求，在软件出现故障之后，要在一定的时间内进行切换，这样才能尽可能小地减少软件发生故障对系统和试验流程的影响。在代码设计过程中，如上文所述将心跳信号为主备切换的依据，代码设计的时候，在发生长时间的心跳信号消失或者是心跳信号跳变，那么在进行判断之后如果确实符合主备切换的条件，则立即进行软件中主备切换模块的函数调用，中间不进行任何不必要的执行过程，以节省切换的时间。除此之外，在心跳信号接收和解析部分的代码中，网络数据的处理上也采用延迟最低的一级缓存模式，采用两个独立的线程，其中一个进行心跳信号数据的接收和存储，另外一个线程进行心跳信号的处理，网络数据只经过一次缓存，最大限度地减少处理数据过程中的时间消耗。而在热备冗余系统设计完成之后，进行系统的切换试验，首先在所内实验室中进行人工计时的方式记录软件切换的时间，记录结果为切换时间在 1 秒之内。为了更精确的进行切换时间的对比，在代码设计中添加心跳信号的发送时间戳、接收时间戳和切换时间戳的记录并保存在本地文件中，在试验结束之后，进行接收时间戳和切换时间戳的比对，得到的结果为实际切换时间约为 0.7 秒。表 3 是在 6 种故障类型完成之后，心跳信号的 3 种时间戳记录表，表中的数据是从主备前置测控软件的心跳信号本地存盘文件中获取的，从表 3 也可以看出，这 6 种故障类型下，主备前置测控软件的实际切换时间为 0.7 秒左右，能够很好地满足目前运载火箭地面测发控系统的试验要求。

表 3　心跳信号时间戳记录表

故障详细情况	心跳信号发送时间戳	心跳信号接收时间戳	主备软件切换时间戳	切换时间/ms
前置测控软件异常退出或者宕机	20:32:16:813	20:32:11:55	20:32:16:766	711
	20:38:25:451	20:38:25:712	20:38:31:435	723
	20:47:38:559	20:47:38:850	20:47:44:552	702
前置测控组合网卡故障	21:11:28:662	21:11:28:923	21:11:34:638	715
	21:20:52:261	21:20:52:521	21:20:58:209	688
	21:25:33:525	21:25:33:763	21:25:39:455	692
前置测控组合通信网线物理损坏	20:52:16:592	20:52:16:817	20:47:23:499	682
	20:57:52:612	20:57:52:873	20:57:58:590	717
	21:06:47:706	21:06:47:963	21:06:53 :689	726
PXI 硬件板卡检测到数据边界值溢出	17:22:52:559	17:22:52:796	17:22:52:559	725
	17:31:12:362	17:31:12:623	17:31:13:341	718
	17:39:38:177	17:39:38:432	17:39:39:115	683
PXI 硬件板卡控制接口返回值不正确	17:02:27:189	17:02:27:426	17:02:28:113	687
	17:09:15:872	17:09:16:127	17:09:16:838	711
	17:15:38:522	17:15:38:784	17:02:39:487	703
PXI 硬件板卡初始化失败	16:36:52:288	16:36:52:541	16:36:53:226	685
	16:42:58:165	16:42:58:416	16:42:59:114	698
	16:55:07:423	16:55:52:681	16:55:53:387	706

5　结束语

设计完成的软件系统具备了在线热备自主切换的能力，能够实现故障之后不需要人工进行软件切换。在系统开启后，主机控制软件也可以根据实际情况修改不同计算机上的软件的主备优先级。软件冗余系统可以对主备软件运行状态进行实时监测，如果出现软件故障可以及时发现并采取处理。主备前置测控软件之间通过状态同步、故障监测和状态切换能实现双机热备冗余系统，每个前置测控软件都具备自检功能，可以根据自身和系统的当前状态确定主备状态。通过试验验证，确定在发生故障之后，3 秒钟之内完成软件的主备切换，并且故障软件的工作状态信息也能进行保存，保证了主备软件工作的连续性和准确性，提升了运载火箭地面测发控软件系统的稳定性。

（下转第 100 页）