http://www.avionicstech.com.cn avionicstech@avic.com

DOI:10.12175/j.issn.1006-141X.2022.01.06

面向综合 CNI 系统的双机热备份切换方案设计

段冰冰，王 涛，张立松

（中国航空无线电电子研究所 , 上海 200241）

[摘 要] 本文针对综合 CNI 系统主备切换功能的实现，提出了一种基于表决算法的双机热备份主从模式的设计方案，从设计思路、设计原则以及冗余备份、主备切换的故障故障检测等方面进行详细分析，对上电确定主备流程、主切备流程以及备切主流程进行详细设计，通过方案验证，在不增加硬件基础上，能够快速无缝地将相应的功能控制切换至备模块，提高了整个综合 CNI 系统的可靠性，保障系统不间断运行。

[关键词] 综合 CNI；冗余备份；故障检测；双机热备份

[中图分类号]TP302.8 [文献标识码]A [文章编号]1006-141X(2022)01-0030-07

Design of Dual-System Hot Backup Switching Scheme for Integrated CNI System

DUAN Bing-bing，WANG Tao，ZHANG Li-song

(China National Aeronautical Radio Electronics Research Institute, Shanghai 200241, China)

Abstract: Aiming at the implementation of the master-slave switching function of the integrated CNI system, a design scheme of the master-slave mode of dual-system hot backup is proposed based on the voting algorithm, and the redundancy backup, design idea, design principles and fault detection of main standby switching are analyzed. It also designs the main and standby procedures for power-on determination, main cut and standby, and main standby cut. Through the verification of the scheme, the corresponding function control can be quickly and seamlessly switched to the standby module without increasing the hardware, which improves the reliability of the whole integrated CNI system and ensures the uninterrupted operation of the system.

Key words: integrated CNI system; redundancy backup; fault detection; dual-system hot standby

通信、导航、识别（CNI：Communication, Navigation & Identification）系统是当代航空电子信息系统中的典型代表系统，随着软硬件技术的高速发展，系统设计逐步采用综合化、开放式的架构。综合化的 CNI 系统设计相对于分立式的传统的 CNI 系统设计而言，采用开放式的体系架构，使得系统具备可扩展性、易插入性和易迭代性，从而延长装备的寿命周期。综合化的 CNI 系统设计分别在结构设计、模块通用化设计、总线选型等方面遵循开放式的思想。其系统组成示意简图如图 1 所示。

综合 CNI 系统由天线及两个机架组成：一个综合射频机架和一个天线接口单元机架，在结构上均采用通用化、开放式的设计。所有的模块均采用现场可更换模块（LRM：Line Replaceable Module）结构，大部分的模块采用通用化的类设计，类内可以实现任意互换。这种基于标准模块的设计，加上统一的总线接口设计，使得 CNI 系统具备了基于模块的动态资源配置、动态故障重构及双机备份切换的能力。

收稿日期：2021-07-08

引用格式：段冰冰，王 涛，张立松 . 面向综合 CNI 系统的双机热备份切换方案设计 [J]. 航空电子技术 ,2022,53(1)： 30-36.

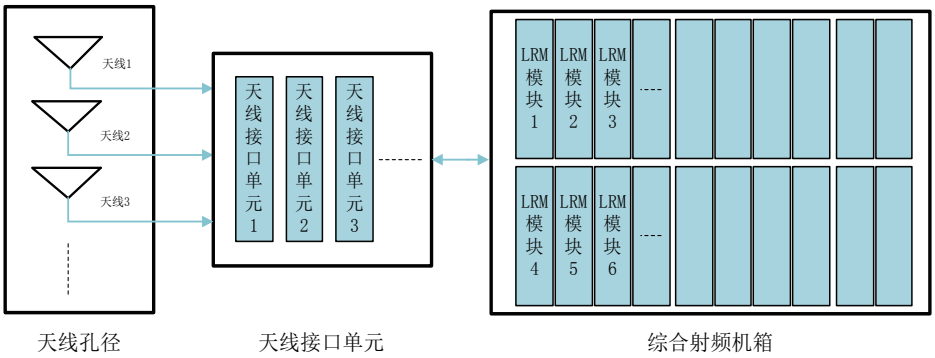

图 1 综合化 CNI 系统组成示意简图

受飞机总体设计要求，机载综合 CNI 系统在重量、体积等方面都有严格的设计限制，因此在不增加硬件的基础上，如何尽可能提高计算机系统的任务可靠性，成为机载综合化的一个重要课题。为保证核心功能的正常运行，常常采用双机备份方法提高系统的可靠性，当主机故障时，能够无缝切换至备机，确保系统能够长期稳定运行。本方案基于某型综合 CNI 系统，为保障系统的生命周期和任务完成度，该系统配置两个主控管理模块，其功能完全相同，互为备份。当主模块故障时，备模块能够快速接管主模块的功能，实现无缝切换，保证综合 CNI 系统的稳定运行。

1　双机冗余备份概述

在实际的工程应用中，双机冗余备份一般采用双机冷备份、双机温备份、双机热备份主从模式和双机热备份双工模式 4 种模式，其拓扑结构如图 2 所示。

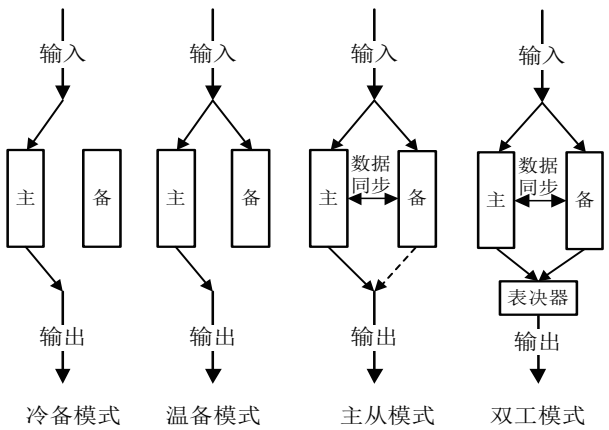

图 2 4 种工作方式拓扑结构

双机冗余备份 4 种工作特点如表 1 所示。一般而言，冷备模式主要适用于冗余备份模块可手动切换的应用工程，但系统的冷备份又存在切换时间太长、延误任务时机的问题，不符合控制实时性要求。温备份模式则适用于无对系统可用度不高的应用工程。而对于双机热备切换主从模式和双工模式则适用于系统可用度较高和实时性较强的应用过程。其中，双工模式能够通过结果比较来及时确定输出方，确保了系统的连续工作，但是该模式要求所有冗余模块必须严格同步，同时表决器设计也比较复杂，随着表决器工作时间的增长，其仲裁可靠度逐渐降低。而主从模式则设计相对简单，当备计算机通过检测到主控计算机故障时，能够通过仲裁将发生故障的主控计算机隔离，使备计算机变为主控计算机，行驶控制职能。

2　双机热备份切换流程设计

为了保证双机冗余系统的高可靠性，同时尽可能降低模块设计复杂度，本文提出了一种面向综合 CNI 的双机热备切换主从工作模式，可根据软硬故障检测达到表决器的效果，模拟实现全双工工作的设计方法，保证系统高效正常运行。

2.1 系统方案设计思想

综合 CNI 系统有两个主控接口管理模块，两个模块同处一个串行总线 RapidIO（SRIO：Serial RapidIO）交换网络如图 3 所示，SRIO 网络只能初始化配置一次，且只能由主模块进行初始化配置。系统正常工作时，优先使用主控模块 1，当系统运行发生关键软硬件故障时进行第一次切换。主控模块 2 不能使用 1553 B 总线对外收发数据，因而系统对外总线顺序优先级为主控模块 1FC 总线 > 主控模块 2 FC 总线 > 主控模块 1 1553 B 总线，当两块主控模块的 FC 总线均出现故障且主控模块 1 没有其他关键软硬件故障时，进行第二次切换，因此为了达到动态双机切换的目标，增加两块主控模块间的总线状态标识同步信息，作为双机热备份切换时的判断条件。

表 1 4 种工作方式工作特点

工作方式	初始主机状态	初始备机状态	工作特点
冷备模式	上电，工作	待加电	主机故障时备机上电接管工作，原主机下电转为冷备份
温备模式	上电，工作	上电，待工作	主机故障时备机立即接管工作，原主机转为待工作状态
主从模式	上电，工作	上电，工作	仅主机对外输出备机状态同步，当主机故障时，备机接管工作原主机转为备份
双工模式	上电，工作	上电，工作	主备机均工作，对外输出时，通过表决器表决后，选择相应计算机进行输出

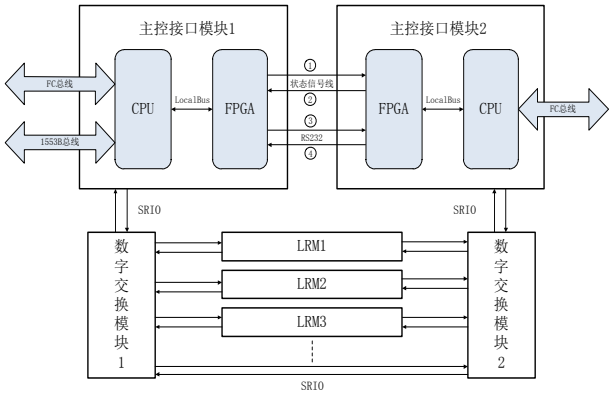

图 3 双主控之间的总线连接示意图

在双主控之间的总线连接示意图中 1 号和 2 号为单向的模块状态信号线，一根只读，一根可设置。通过高低电平表征模块的正常、异常状态，如果是“高”，代表模块故障（ERROR）；如果是“低”，代表模块正常（OK）。CPU 可通过 LocalBus 总线读取或设置状态信号线的电平。CPU 周期性的通过 LocalBus 向 FPGA 发送或读取模块状态，模块状态正常时发送 0，模块故障时发送 1，FPGA 在收到 0 时将离散线电平拉低，FPGA 在收到 1 时将离散线电平拉高。FPGA 间两根状态信号线初始为“高”状态，系统管理软件通过自检结果确定主控模块为正常状态后，必须首先设置信号线为“低”，以向另外一个主控模块表明本模块状态正常。在系统管理软件通过自检结果确定主控模块为异常状态后，状态信号线会被拉“高”，以向另外一个主控模块表明本模块状态异常。在 CPU 故障、主控接口模块不在位、系统管理未发送 0 时，状态信号线的状态都为“高”。

2.2 系统方案设计原则

（1）综合 CNI 机架内部采用 SRIO 总线网络，系统首次上电时由主模块进行 SRIO 网络路由配置，在系统掉电之前不再进行 SRIO 网络路由配置。主备切换是指对 SRIO 网络的使用权，主模块“既收又发”，通过 SRIO 总线收发内部数据，通过 FC、1553B 总线收发外部数据；备份模块对外“只收不发”，通过 FC 总线接收外部数据，不对外发送数据，不使用 SRIO 收发内部数据；

（2）主模块和备模块之间通过离散线高低电平确认对方模块状态，默认是“高”，如果是“高”，代表对端模块故障（ERROR）；如果是“低”，代表对端模块正常（OK）；

（3）主模块和备模块之间通过 RS232 串行接口同步信息，包括主备状态、总线状态标识、故障信息等；

（4）为保证网络中不会存在两个主模块，主模块只有满足以下两种方式确认是否切换为备：本模块出现关键软硬件故障，将本模块状态设置为“ERROR”；备份模块状态为“OK”（主控模块 1 为主时）或备份模块状态为“ERROR”且总线状态标识为“OK”（主控模块 2 为主时）；

（5）主控模块 1 最多进行初始化时的备切主、运行时故障主切备和只有 FC 总线故障时备切主的三次切换；主控模块 2 模块最多进行两次切换，备切主的切换和主切备的切换。

2.3 综合化 CNI 的故障模式与影响分析

综合 CNI 系统集通信、导航、识别功能于一体，采用开放式系统架构，以模块化、通用化、软件化实现全系统的综合化。综合 CNI 主备切换所涉及的故障模式按照故障检测方式分为软件可检测故障和软件不可检测故障。

2.3.1 软件可检测故障

软件可检测故障主要指主控系统管理软件可以检测到的故障，如 FC 通信故障、1553B 总线通信故障、SRIO 链路故障、FPGA 故障、CPU 故障和接口管理软件故障等。其软件可检测故障列表如表 2 所示。

在系统管理软件上电自检或周期自检通过调用检测函数，读取软件可检测故障检测函数状态，当检测函数的返回值异常时则应考虑主备切换。对应处理为系统管理软件将本模块状态置为“ERROR”，调用底层驱动接口，通过 LocalBus 总线将状态信号线的电平拉“高”，同时若没有其它故障将总线状态标识置为“OK”。

表 2 六软件可检测故障

故障名称	检测函数名称	检测函数状态	本模块状态
FC 通信故障	FC 子卡驱动函数	返回值异常	ERROR
1553B 总线通信故障	MBI 检测接口函数	返回值异常	ERROR
SRIO 链路故障	SRIO 检测接口函数	返回值异常	ERROR
CPU 故障	CPU 检测接口函数	返回值异常	ERROR
FPGA 故障	FPGA 检测接口函数	返回值异常	ERROR
接口管理软件故障	心跳检测函数	无上报	ERROR

2.3.2 软件不可检测故障

软件不可检测故障，是指由于系统管理软件本身故障，导致系统管理软件无法正常监控模块状态的情况。出现上述情况，应该通过模块硬件看门狗复位，来使得主控接口模块的状态恢复为“ERROR”。因此，主控接口模块中的系统管理软件应在完成初始化后，启动模块硬件看门狗，并周期执行喂狗操作。

2.3.3 故障模式与影响分析

综合 CNI 系统的功能电路是由统一标准机箱和标准模块进行设计，系统中核心功能关键点采用二模块冗余热备份，其重构方式包括任务重构和故障重构。综合化 CNI 的故障重构，即通用资源发生故障后，系统按照功能优先级进行资源重构，使系统具有容错能力，故障重构的过程包括故障侦测、故障隔离、程序加载、主备切换。本文中面向综合 CNI 的双机热备切换主从工作模式，是由系统管理软件对系统运行进行全周期检测，根据软件可检测故障与不可检测故障上报，系统管理软件对于不同的故障模式分配不同优先级，通过主备 422 总线发送给对端模块，主模块与备模块同时对产生的故障模式进行影响分析，将收集到的故障状态设置故障标志位。通过软硬件检测的故障标志位进行表决器加权模拟，确保能够实时监测触发主备切换的故障模式，提高系统主备切换的稳定性。

2.4 热备份主备切换设计

2.4.1 主备模块数据同步设计流程

系统正常运行时，主模块和备模块上的系统管理软件需要将本模块的状态信息数据传输给对端模块，其中状态信息数据包括总线状态标识数据、本模块的主备状态、故障信息、方案号、资源配置信息等相关数据。为了保证主备模块之间数据传输的可靠性，本文使用结构体指针来实现 RS422 总线数据无损和可靠传输，其设计流程如图 4 所示。

该设计利用结构体指针，将主备之间所传数据装入定义好的数据结构中，发送方定义指向该结构体的字符指针，按字符型数据结构将该结构体中数据拆分出来，单个字节调用 422 数据传输接口将数据发送出去。接收方在收到 422 数据后，利用接收数据结构体指针将接收到的数据依次装入到数据结构体中，按发送方数据结构组装成相同的数据体，保证了实际接收的数据和发送的数据相同。

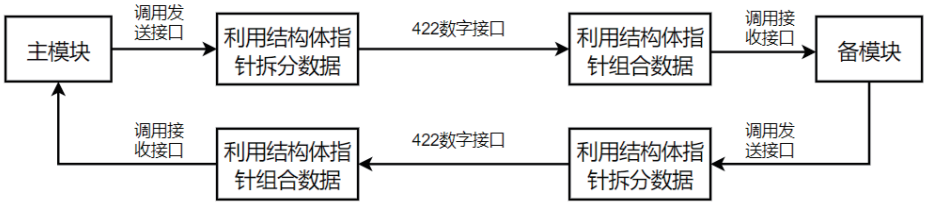

图 4 主备模块数据同步设计流程图

2.4.2 主模块切换备模块流程

系统正常运行过程中主模块切为备模块的流程如图 5 所示，主模块切换备模块则是利用主控模块间周期备份信息、切换次数、本模块状态和总线标识以及对端模块状态和总线标识等数据进行逻辑判断，从而将主模块标志位由主切换为备。

首先，主控模块将本模块周期自检、周期发送备份信息和总线状态标识给对端模块，本模块状态为 OK，对端模块状态为 OK，切换次数为 0 的情况下，如果槽位号不为 1，则切换至备状态，否则维持主状态。其次，当本模块状态为 ERROR，槽位不为 1 的情况时，无需判断对端模块状态，主备的标志位均切换至备状态。最后，槽位等于 1 的情况时，对端模块状态 OK 则切换至备状态，无论本模块总线标识是否 OK 均维持主状态。

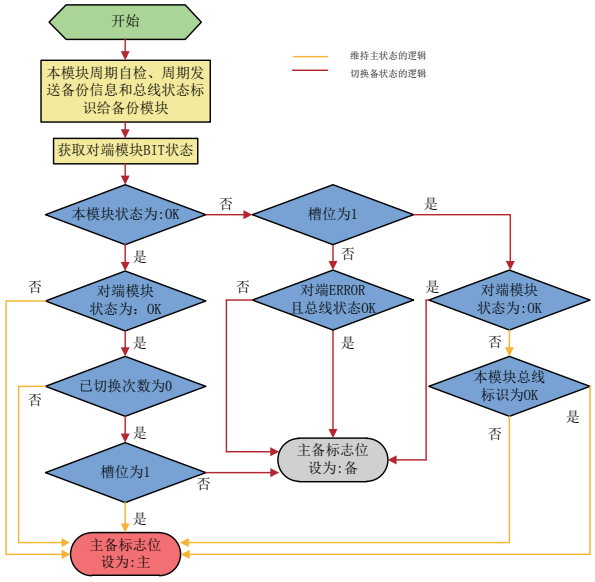

图 5 主模块切为备模块的流程图

2.4.3 备模块切换主模块流程

系统正常运行过程中备模块的状态位由备切换为主的流程如图 6 所示，备模块切换到主模块则是利用主控模块间周期备份信息、切换次数、本模块状态和总线标识以及对端模块状态和总线标识等数据进行逻辑判断，从而将主模块标志位由备切换为主。

首先，主控模块将本模块周期自检、周期发送备份信息和总线状态标识给对端模块，本模块状态为 OK，对端模块状态为 ERROR，则切换为主状态；对端模块状态为 OK，切换次数为 0 的情况下，如果槽位号为 1，则切换为主状态，否则维持备状态。

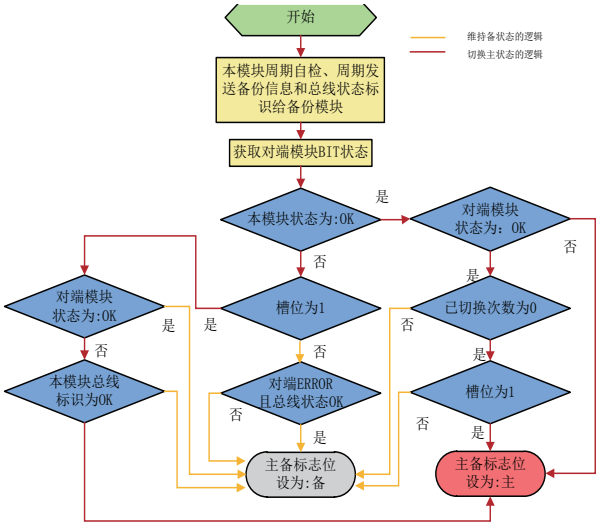

图 6 主模块切为备模块的流程图

其次，当本模块状态为 ERROR，槽位不为 1 的情况时，无需判断对端模块状态，主备的标志位均切换至备状态。最后，槽位等于 1 的情况时，对端模块状态 OK 则均维持备状态，若本模块总线标识是否 OK 情况下切换为主状态，否则均维持备状态。

2.5 双机切换方案验证

通过对本方案设计思路、原则、故障检测以及主备切换的分析与设计，制定了图 7 完整的双机热备份切换流程图。在实际运行环境过程中，综合 CNI 系统进行双机热备份切换的验证包含硬件故障检测切换和软件故障检测切换，分别对其进行模拟验证。

2.5.1 硬件故障检测验证

对以下几种可模拟硬件故障的实际应用场景进行综合 CNI 系统进行双机热备份切换的方案验证：

场景 1：双主控状态正常，FC 总线，1553 B 总线正常，系统正常上电；

场景 2：主控 1 状态正常，主控 2 状态异常 (模块拔除)，FC 总线，1553 B 总线正常，系统正常上电；

场景 3：主控 2 状态正常，主控 1 状态异常 (模块拔除)，FC 总线，1553 B 总线正常，系统正常上电；

场景 4：双主控状态正常，FC1 总线正常，FC2 总线异常（总线拔除），1553 B 总线正常，系统正常运行；

场景 5：双主控状态正常，FC2 总线正常，FC1 总线异常（总线拔除），1553 B 总线正常，系统正

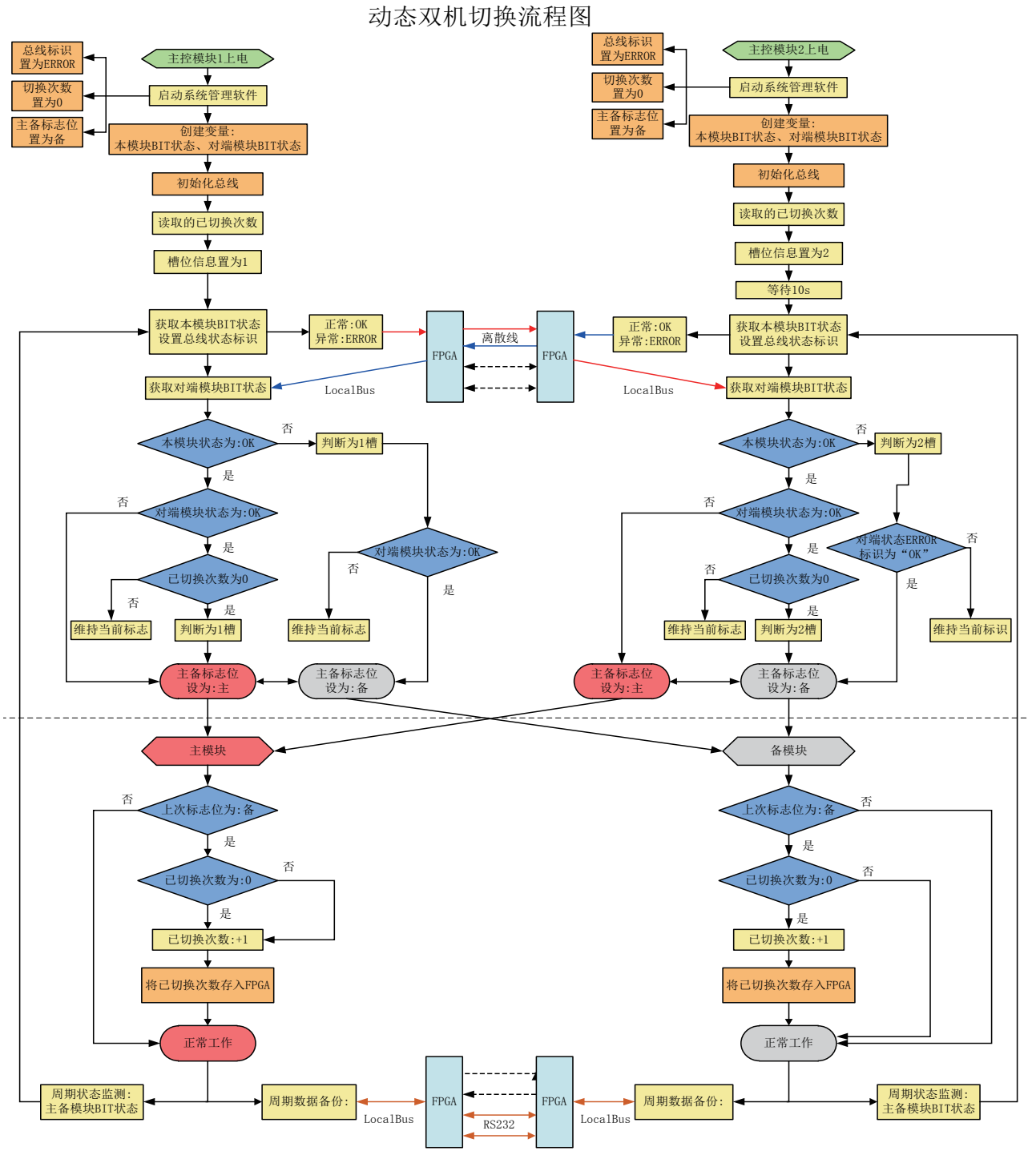

图 7 完整的双机热备份切换流程图

正常运行；

场景 6：双主控状态正常，FC1，FC2 总线异常（总线拔除），1553 B 总线正常，系统正常运行。

利用综合 CNI 机箱分别对以上硬件可实现故障场景进行方案验证，其中双备份主控模块可通过拨出的方式模拟其飞行过程中硬件故障的状态，FC、1553 B 等总线故障通过其断开连接方式模拟其硬件故障状态，其验证结果如表 3 所示。

表 3 六种场景主备切换结果

场景	是否发生切换	切换前主标识位	预期主标识位	实测切换主标识位
场景 1	否	主控 1	主控 1	主控 1
场景 2	否	主控 1	主控 1	主控 1
场景 3	是	主控 1	主控 2	主控 2
场景 4	否	主控 1	主控 1	主控 1
场景 5	是	主控 1	主控 2	主控 2
场景 6	是	主控 1	主控 1	主控 1

同时主备切换过程的验证不仅仅涉及逻辑切换是否正确，还需包含完成切换的时间以及多次验证切换的正确率，因而在同一场景下分别进行 20 次上下电进行其切换效率的测试，通过对观测开始切换波形参数上报消失到切换完成波形参数上报恢复来记录切换时间差，其验证结果如表 4 所示。

表 4 六种场景下多次主备切换结果

场景	场景验证次数	平均切换时间 /s	切换准确率
场景 1	20	0	100%
场景 2	20	0	100%
场景 3	20	5.35	100%
场景 4	20	0	100%
场景 5	20	5.78	100%
场景 6	20	6.24	100%

2.5.2 软件故障检测验证

对以下几种可模拟软件故障的实际应用场景进行综合 CNI 系统进行双机热备份切换的方案验证：

场景 1：双主控状态正常，针对 SRIO 检测接口函数，通过 shell 强制写入 ERROR，系统正常上电；

场景 2：双主控状态正常，针对 CPU 检测接口函数，通过 shell 强制写入 ERROR，系统正常上电；

场景 3：双主控状态正常，针对 FPGA 检测接口函数，通过 shell 强制写入 ERROR，系统正常上电；

场景 4：双主控状态正常，针对心跳检测函数，通过 shell 强制写入 ERROR，系统正常上电。

利用综合 CNI 机箱分别对以上模拟软件故障场景进行方案验证，输入软件模式返回值后，通过打印切换后主备标志位值的变化来确认是否切换成功，通过打印切换过程 tickGet() 时间差来记录软件主备切换时间差，其验证结果如表 5 所示。

表 5 四种场景下多次主备切换结果

场景	是否发生切换	场景验证次数	平均切换时间 /ms	切换准确率
场景 1	是	20	53	100%
场景 2	是	20	56	100%
场景 3	是	20	57	100%
场景 4	是	20	51	100%

3 结论

本文通过综合 CNI 系统设计引入双机冗余备份切换，介绍了不同冗余备份的工作特点，提出了一种全双工工作的热机备份设计方案，并从设计思路、设计原则以及主备切换的故障故障检测等方面进行了方案设计。本方案已应用在了某综合化 CNI 系统中，通过试验与联试过程的验证，证明在主模块功能部分或全部失效情况下，该方案能够快速无缝地将相应的功能控制切换至备模块，提高了整个综合 CNI 系统的可靠性。

参 考 文 献

[1] 顾生辉 . RapidIO 在综合化 CNI 系统中的应用 [J]. 计算机与网络 , 2015, 54(4): 51-54.

[2] 赵豫峰 , 张善从 . 一种双机热备的嵌入式计算机系统设计 [J]. 国外电子测量技术 , 2013, 32(5): 75-78.

[3]Luo Y, Tao R, Zhao M, et al. Design and realization of synthetic control equipment based on dual hot redundancy technology[J]. Modern Defense Technology, 2018.

[4] 张科超 , 崔刚 . 实时嵌入式系统中的双机热备份容错设计 [J]. 计算机研究与发展 , 2010, 47(S): 133-136.

[5] 吴娟 , 马永强 , 刘影 . 一种基于主备机快速切换的双机容错系统 [J]. 计算机应用 , 2005, 38(3): 52-25.

[6] 丁瑞 , 张士化 , 董恒贝 , 等 . 一种基于高速数据交换的强实时性双机同步容错系统 , CN109739697A[P]. 2019.

[7] 李兴玮 , 潘玉林 , 黄柯棣 . 基于 422 串口的无损数字通讯方法 [J]. 计算机工程与设计 ,2005, (7): 1808-1809+1818.