

文章编号: 2097-597X(2025)06-0011-007

DOI: 10.26917/j.cnki.issn.2097-597X.2025.06.002

基于单一数据节点的系统网络冗余备份方法研究

王炯超*, 黎明, 敬鸿飞

中电科航空电子有限公司, 成都 611731

摘要: 现代飞机的机载系统自动化与集成化程度非常高, 机载系统的可靠性对飞机的飞行安全有着重大影响。提高机载系统的安全性有很多方法, 如提高硬件设备本身的防护等级、可靠性, 或者采取冗余设计等。文章主要采用系统冗余设计来提升机载网络通信管理子系统的安全性与可靠性, 首先阐述了主备用服务器切换的网络模型, 介绍了网络冗余算法以及系统故障探测算法, 最后通过模拟设备搭建实验网络环境, 对冗余备份的切换网络方案进行验证。

关键词: 可靠性; 安全性; 冗余设计; 主备切换; 故障探测

Research on system network redundant backup method based on single data node

Wang Jiongchao*, Li Ming, Jing Hongfei

China Electronic Technology Corporation Avionics, Chengdu 611731, China

Abstract: The degree of automation and integration of aircraft onboard systems is increasing, and the reliability of onboard systems has a significant impact on the flight safety of the aircraft. There are many methods to improve the security of airborne systems, such as improving the protection level and reliability of hardware equipment itself, or adopting redundant design. This article mainly adopts system redundancy design to enhance the security and reliability of the airborne network communication management subsystem. Firstly, this article introduces the network model for switching from primary servers to backup one or vice versa, introduces network redundancy algorithms and system fault detection algorithms. Finally, a laboratory network environment was established through simulation equipment to verify the switching network scheme of redundant backup system.

Keywords: reliability; security; redundant design; master backup switching; fault detection

收稿日期: 2025-05-21

修订日期: 2025-06-10

作者简介: 王炯超(1984年生), 男, 硕士, 工程师; 主要研究方向为民用飞机空地通信;

*通信作者, E-mail: wangjc@cetca.net.cn

黎明(1977年生), 男, 硕士, 高工; 主要研究方向为航空电子、计算机软件与理论

敬鸿飞(1986年生), 男, 本科, 工程师; 主要研究方向为民用飞机空地通信

0 引言

随着民用航空运输业的飞速发展，航空机载电子系统正快速步入信息化、网络化的时代，未来的民航运输业务将在真正意义上实现空地互联互通，机载业务也将通过L、Ka、北斗卫星链路、ACARS、ATG、AeroMACS、LDACS等通信链路接入地面网络。机载网络通信管理子系统(network communication management sub-system, NCMS)正承载着管理复杂空地通信链路的使命，该系统可以实现对空地多链路集中管控，实现业务接入控制、动态路由决策、自适应流量控制(AEEC, 2014a)以及安全可靠传输(AEEC, 2014b)，正是由于网络通信管理子系统具有举足轻重的作用，因此对其安全性与可靠性提出了更高的要求。传统解决系统可靠性的方法可以通过克隆关键设备，形成双冗余备份，从而提升系统的可靠性，然而这种冗余备份往往需要两路独立的数据输入主/备设备，在很多民航确定构型下是无法获得多节点数据输入的，因此本文通过对机载网络通信管理子系统进行冗余设计来研究基于单一数据节点的系统网络冗余备份方法。

1 检测模型框架

1.1 虚拟化冗余技术

虚拟化冗余技术是将多台物理设备虚拟为

一个设备组，对于其他设备来说，该设备组具有唯一的设备IP(张友凯等, 2020)，可以适用于更多的网络场景，通常用在网关设备中。虚拟路由器冗余协议(virtual router redundancy protocol, VRRP)是最常用的协议之一，用于实现网关的高可用性，使得在一台网关设备宕机时，另外一台备份设备可以无缝接管，从而不会造成业务中断，以提高网络服务质量(李冬洋和严勇, 2021; 王涛, 2022)。

1.2 主备服务器切换原理

本设计方案基于某型机载系统构型，在该系统构型下客舱电子系统中各关联子系统均只能发出一路数据到网络通信管理子系统，因此客舱各电子子系统数据流只能从网络通信管理服务器(network communication management server, NCMS)的交换板接入，当服务器失效时，数据需要通过该服务器的交换板转发到备用服务器进行数据处理，主备切换实现方案如图1所示。

如图1所示，为实现主备服务器间数据交互，通过以太网线连接主备服务器的两个通信端口，并将这两个端口设置为trunk口，从而实现跨交换机的VLAN通信(Li et al., 2023; Zhang et al., 2024)。

NCMS主备切换不仅需要主备服务器作为运行主体进行功能切换，还需要在切换时将输入系统的数据流进行切换。为了在主服务器运行

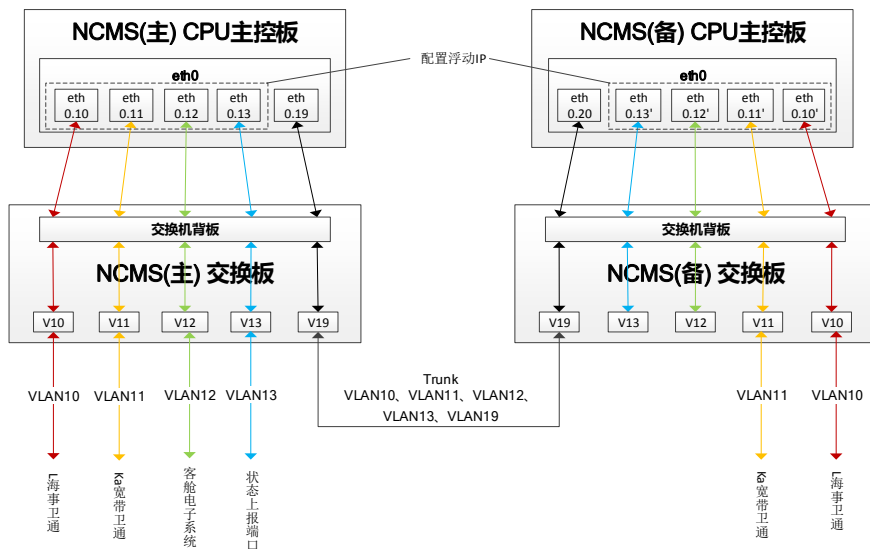


图 1 NCMS 服务器主备切换数据流

故障时,将业务流从主服务器切换到备用服务器,本方案采用浮动IP配置。在NCMS主控板的eth0端口上根据业务流划分虚接口,同理,在备用服务器上进行相同的VLAN划分,然后针对主备服务器上的同一业务流的虚接口分别配置浮动IP,比如针对eth0.10和eth0.10'两个虚接口配置浮动IP为10.10.10.10。在正常工作模式下(eth0.10激活,eth0.10'去激活),IP地址10.10.10.10指向eth0.10接口,当主服务器失效后(eth0.10去激活,eth0.10'激活),IP地址10.10.10.10指向eth0.10'接口,但是这里需要注意子接口激活/去激活的操作顺序。为避免出现IP地址冲突,需要先去激活故障侧的业务子接口,然后再激活将接管业务侧的子接口。

2 网络冗余算法

2.1 冗余处理逻辑

NCMS主备服务器中均驻留冗余模块,冗余模块的业务处理逻辑根据主备服务器的运行状态不同而变化。

2.1.1 主服务器(“Service”状态)

- (1) eth0.10、eth0.11、eth0.12、eth0.13、eth0.19子接口状态为UP。
- (2) 运行网络通信管理软件。
- (3) 周期检测网络通信管理软件运行状态。
- (4) 网络通信管理软件运行异常时,主动发起切换流程。

2.1.2 备用服务器(“Free”状态)

- (1) eth0.10'、eth0.11'、eth0.12'、eth0.13'子接口状态为DOWN。
- (2) eth0.20子接口状态为UP。
- (3) 系统监测主备服务器之间的心跳。
- (4) 实时监听对端切换请求事件。

在整个系统运行过程中,必须确保主备服务器所维护的系统状态统一。

2.2 冗余切换模式

2.2.1 触发切换模式(邵忠俊等,2021;唐成等,2021)

(1) 主动触发模式。主服务器中驻留冗余模块,周期监测本端软件运行状态,当发现软件

运行异常时,立即触发“切换请求”消息发送到备用服务器,完成主备切换。

(2) 被动触发模式。备用服务器向主服务器周期性查询软件运行状态,当发现软件运行异常时,立即触发“切换命令”消息发送到主服务器,完成主备切换。

2.2.2 模式选择

(1) 主动触发模式的优点。时效性比较好,冗余模块发现异常即可触发主备切换流程。被动触发模式中当冗余模块发现异常后,需要被动等待对端周期查询到来才能触发切换流程,如果查询周期太长,用户层面感知不好;如果查询周期太短,会对系统负载产生一定影响(Zhang et al., 2018)。

(2) 主动触发模式的缺点。针对以下两种异常场景,主动触发模式无法感知,不能完成正常切换。①主服务器冗余模块本身异常,导致软件运行异常时无法发出“切换请求”;②主备服务器之间通信故障,主服务器发出的“切换请求”无法被接收。

被动触发模式可以感知以上两种异常场景(周期查询无响应),但是主备服务器要完成切换流程,需要依赖于“主备通信”+“冗余模块正常工作”,因此被动触发模式也不能完成正常切换。

2.3 冗余切换流程

综合前述两种模式优缺点分析,选择主动触发模式来实现主备切换(Pamies-Juarez et al., 2013),其切换流程如图2所示,主备服务器切换过程包含两个阶段。

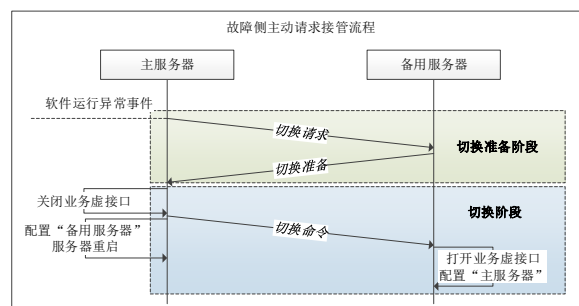


图2 故障侧主动请求切换流程

2.3.1 切换准备阶段

切换准备阶段主要有两个目的：①检测主备服务器之间的连通性，如果主备服务器之间通信不可达，将无法启动切换流程；②检测备用服务器冗余模块是否正常工作，如果备用服务器冗余模块未能正常响应，切换流程也无法执行。

切换准备阶段操作流程如下：①当主服务器检测到网络通信管理软件运行异常时，立即向备用服务器发送“切换请求”；②备用服务器收到“切换请求”后回复“切换准备”。至此切换准备阶段完成，主服务器收到“切换准备”消息后，知道对端已经准备好，就可以启动切

换流程了。

2.3.2 切换阶段

切换阶段操作流程如下(王涛等, 2024):

- ①当主服务器收到备用服务器发来的“切换准备”消息后，立即去激活本端所有业务子接口；
- ②主服务器业务子端口去激活成功后，发送“切换命令”给备用服务器，同时配置本端服务器为“备用服务器”并重启；
- ③备用服务器收到“切换命令”后，打开所有业务子接口，并配置本端服务器为“主服务器”。

冗余模块处理逻辑如图3所示(Renna, 2019; Liu & Tipper, 2013)。

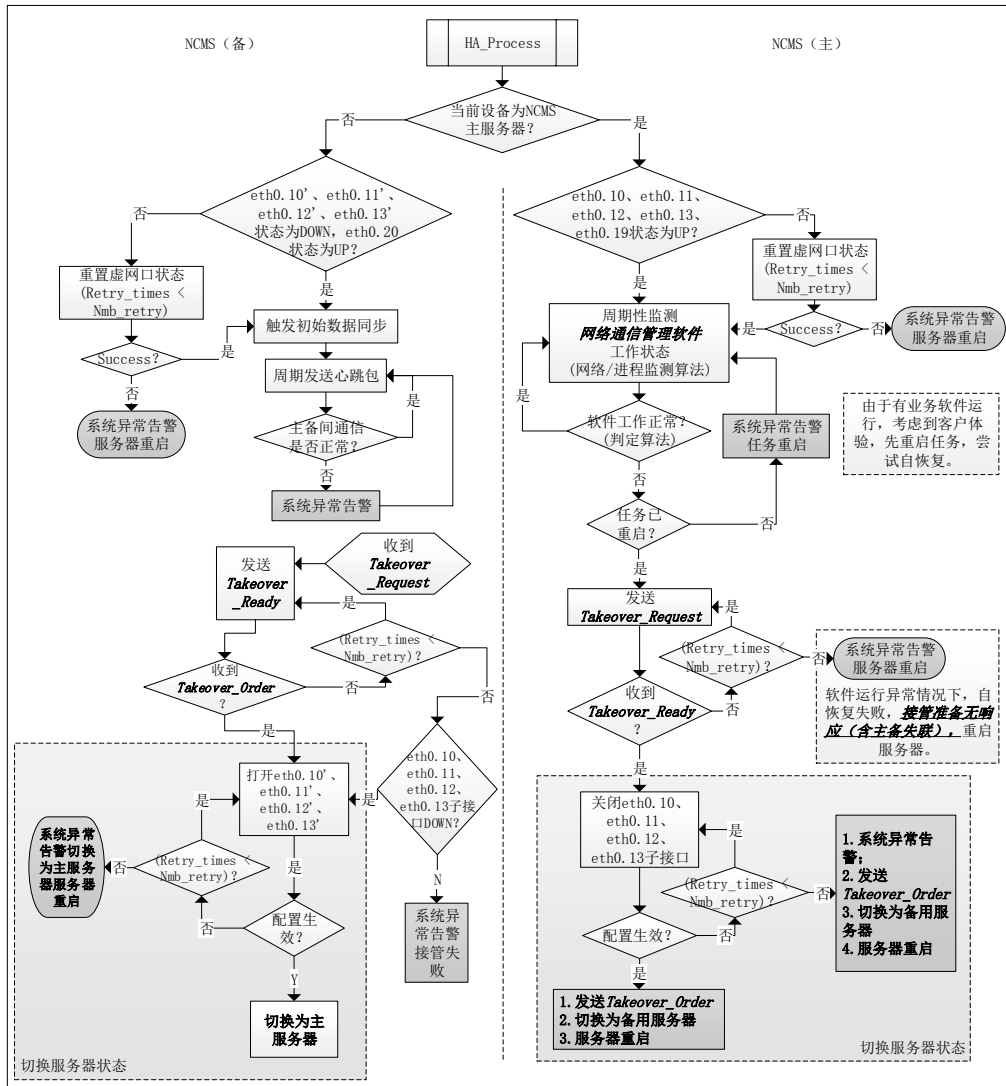


图3 主备切换逻辑

3 切换网络方案验证

在实验室环境下对切换网络方案进行验证,这里对网络方案进行了简化,两台 Windows 主机分别模拟机载端和地面端设备,两台 Linux 主机和两台交换机分别模拟主备服务器,实验室环境物理连接示意图如图4所示。

网络方案验证实验原理:本验证实验通过在机载设备模拟器上推送测试视频流,然后分别在机载设备模拟器、地面设备模拟器上拉取视频流,其中机载设备模拟器上的视频流拉取为网络自环,地面设备模拟器上的视频流拉取需要经过主备服务器的两条主备通信链路。在视频流拉取过程中,通过构造服务器故障以及故障恢复产生的链路切换场景,在这些场景下对比两端不同网络下的视频流拉取结果是否满

足实验要求。

3.1 网络环境配置

3.1.1 机载端模拟器配置

(1) 配置网卡 IP: 192.168.10.5; 网关: 192.168.10.10。

(2) 安装 vlc 播放器。

(3) 安装视频推送软件 MediaServer。

3.1.2 地面端模拟器配置

(1) 配置网卡 IP: 192.168.11.5; 网关: 192.168.11.10。

(2) 安装 vlc 播放器。

3.1.3 主服务器配置

说明:主服务器的 MAC 地址为 00-22-46-

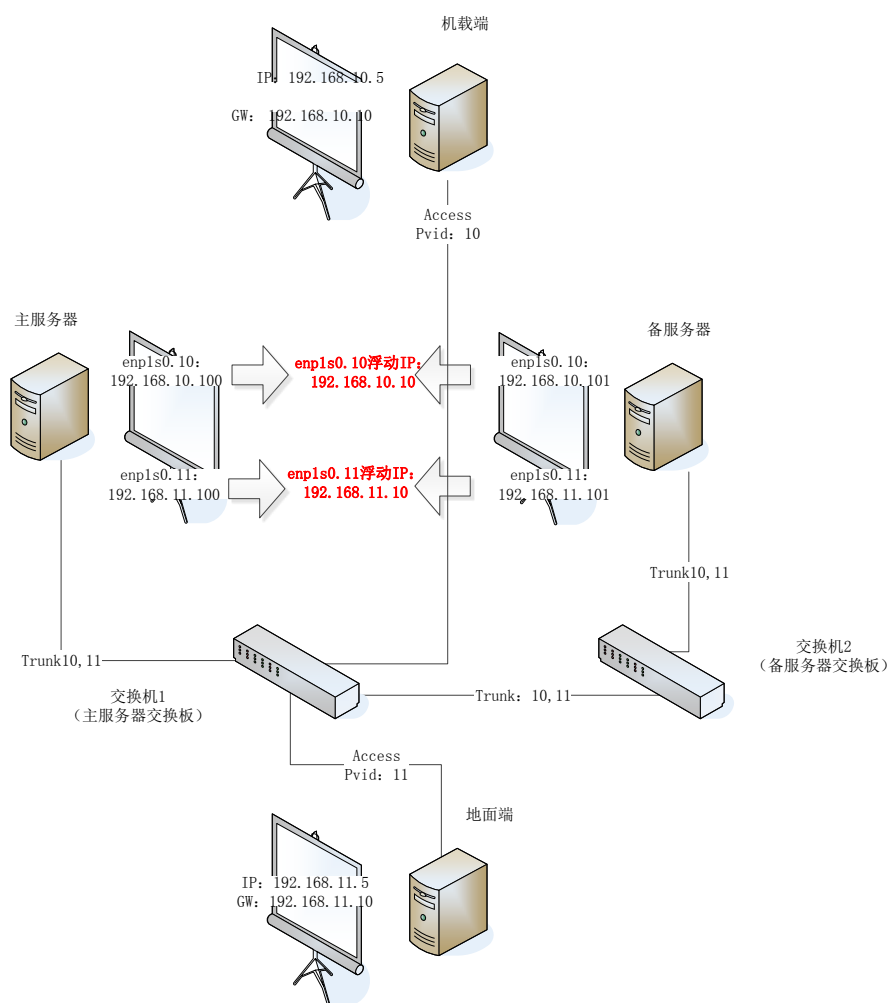


图4 实验室环境建设

4e-28-9c。

(1) 在 enp1s0 上建立两个虚拟网卡 enp1s0.10 和 enp1s0.11，分别配置静态 IP 为 192.168.10.100 和 192.168.11.100，并使能 vlan，enp1s0.11 配置网关 192.168.11.5，并使能默认路由。

(2) 部署冗余模块程序。

(3) 配置冗余模块 state 为 MASTER，配置 enp1s0.10 浮动 IP 为 192.168.10.10，enp1s0.11 浮动 IP 为 192.168.11.10。

3.1.4 备用服务器配置

说明：备用服务器的 MAC 地址为 00-22-46-49-9e-58。

(1) 在 enp1s0 上建立两个虚拟网卡 enp1s0.10 和 enp1s0.11，分别配置静态 IP 为 192.168.10.101 和 192.168.11.101，并使能 vlan，enp1s0.11 配置网关 192.168.11.5，并使能默认路由。

(2) 部署冗余模块程序。

(3) 配置冗余模块 state 为 SLAVE，配置 enp1s0.10 浮动 IP 为 192.168.10.10，enp1s0.11 浮动 IP 为 192.168.11.10。

3.1.5 交换机1(主服务器交换板)配置

(1) Interface 1：连接交换机 2 的 Interface 1 接口，配置 trunk 模式，允许通过 vlan10、vlan11。

(2) Interface 2：连接主服务器 enp1s0 接口，配置 trunk 模式，允许通过 vlan10、vlan11。

(3) Interface 3：连接机载模拟器，配置 access 模式，pvid 为 10。

(4) Interface 4：连接地面模拟器，配置 access 模式，pvid 为 11。

3.1.6 交换机2(备用服务器交换板)配置

(1) Interface 1：连接交换机 1 的 Interface 1 接口，配置 trunk 模式，允许通过 vlan10、vlan11。

(2) Interface 2：连接备用服务器 enp1s0 接口，配置 trunk 模式，允许通过 vlan10、vlan11。

3.2 方案验证

(1) 在主备服务器上均执行 iptables-F 命令，关闭防火墙；启动冗余模块进程。

(2) 在机载模拟器上运行 MediaServer，打开 MediaServer 程序；运行 run.bat，执行推流命令。

(3) 打开 vlc 播放器，通过本地环回网络拉取视频流，用于和地面模拟器上拉取的视频流进行对比；选择媒体→打开网络串流→网络页签，输入 URL：rtsp://192.168.10.5:554/live/1。

(4) 点击播放，成功在机载模拟器上通过环回网络拉流播放视频，同样操作也在地面服务器上完成拉流播放视频，此时通过 arp 信息查看视频流传输路径，192.168.10.10 解析到的 MAC 地址为 00-22-46-4e-28-9c(主服务器)，说明当前视频流通过主链路(主服务器)传输过来。如图 5 所示。



图 5 主备服务器均正常时视频通过主链路正常传输

(5) 此时在主服务器上命令行执行 ifdown enp1s0.10 enp1s0.11，模拟主服务器出现故障，查看 arp 信息及视频播放情况，如图 6 所示，192.168.10.10 解析到的 MAC 地址为 00-22-46-49-9e-58(备用服务器)，说明视频流已通过备用链路传输过来，从视频显示可以看出，经过主备链路切换视频保持流畅播放。

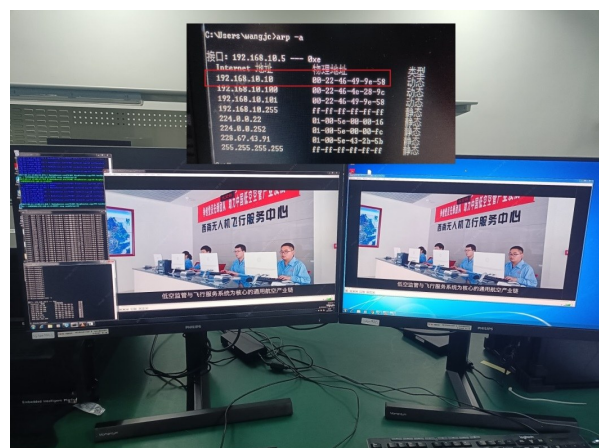


图 6 主服务器故障时视频流切换到备用链路正常传输

(6) 继续在主服务器上命令行执行 `ifup enp1s0.10 enp1s0.11`, 模拟主服务器故障恢复, 查看 arp 信息及视频播放情况如图 7 所示, 192.168.10.10 又重新解析到 MAC 地址 00-22-46-4e-28-9c(主服务器), 说明视频流又回到了主链路上传输, 视频仍然保持流畅播放。



图 7 主服务器故障恢复时视频流切回主链路正常传输

4 结语

本文基于某型机载系统构型设计主备服务器切换网络模型, 并设计网络冗余切换算法, 最后搭建实验室验证环境, 通过两台 Windows 工控机分别模拟机载和地面模拟器, 用两台 Linux 主机和两台交换机分别模拟主备用服务器, Linux 主机模拟服务器主控板, 交换机模拟服务器交换板, 机载端模拟器通过 MediaServer 向地面端模拟器推送视频流, 机载端视频流传输过程, 首先会被发送到网关服务器, 网关服务器收到视频流后经路由策略发送到地面模拟器。测试过程中触发模拟主服务器故障以及故障恢复, 测试表明本网络实施方案可以满足主备服务器故障切换要求。

参考文献:

李冬洋, 严勇, 2021. 一种基于组播机制的双机热备软件系统设计[J]. 现代雷达, 43(1):16-20.

邵忠俊, 营旭东, 秦岭, 等, 2021. 一种高可靠的容错系统设计实现[J]. 中国新通信, 23(5):57-58.

唐成, 潘雷, 刘可昌, 等, 2021. 一种双机热备切换系统的实现方案[J]. 电子世界(22):198-199.

王涛, 2022. 轨道交通信号系统中冗余技术研究[J]. 铁路通信信号工程技术, 19(1):12-15, 23.

王涛, 陈学军, 李泽西, 等, 2024. 一种基于节点同步的热备系统自动运行同步及恢复方法[J]. 电讯技术, 64(12):2024-2031.

张友凯, 贾立辉, 董涛, 2020. 基于虚拟IP的双机热备系统设计及实现[J]. 信息技术与信息化(10):147-149.

AEEC, 2014a. Function definition of airborne manager of air-ground interface communication (MAGIC): ARINC Specification 839[S]. Warrendale: SAE-ITC: 68-70.

AEEC, 2014b. Aircraft/Ground information exchange (AGIE) using internet protocols: ARINC Specification 830[S]. Warrendale: SAE-ITC: 82-85.

LI X Y, LI X P, FENG J X, et al, 2023. Reliability analysis and optimization of multi-phased spaceflight with backup missions and mixed redundancy strategy [J]. Reliability engineering and system safety, 237:109373.

LIU V Y, TIPPER D W, 2013. Spare capacity allocation using shared backup path protection for dual link failures [J]. Computer communications, 36(6):666-677.

PAMIES-JUAREZ L, DATTA A, OGGIER F, 2013. In-network redundancy generation for opportunistic speedup of data backup [J]. Future generation computer systems, 29(6):1353-1362.

RENNA P, 2019. Evaluation of redundant configurations and backup stations to support fault tolerant flow line design[J]. The international journal of advanced manufacturing technology, 101(1/2/3/4):825-837.

ZHANG Y C, ZHU W X, FENG D, et al, 2024. A fragmentation-aware redundancy elimination scheme for inline backup systems[J]. Future generation computer systems, 156(C):53-63.

ZHANG Z H, YIN Y F, ZHANG X, et al, 2018. Optimization of robustness of interdependent network controllability by redundant design [J]. PloS one, 13(2): e0192874.