doi:10.11887/j.cn.201505015 http://journal.nudt.edu.cn

无人机自驾仪硬件加固方案设计与可靠性分析*

郭天豪[1],侯中喜[1],姜晶菲[2],姜汉卿[1]
(1. 国防科技大学 航天科学与工程学院,湖南 长沙 410073;
2. 国防科技大学 计算机学院,湖南 长沙 410073)

摘 要:自驾仪是无人机实现自主飞行与自主完成各项任务的核心器件。现有商用无人机自驾仪大多没有进行硬件加固,直接用来执行重大任务时有一定风险。通过分析可知自驾仪组成模块中对安全性和可靠性影响最大的模块为控制解算器。根据逐步提高的容错需求,使用复位器、计数器、反相器、选择器等简单器件以及在芯片内部添加简单代码,分别设计了单机复位加固方案、双机热备加固方案、硬件切换和软件切换双机互备加固方案。重点研究了加固方案的可靠性随时间的变化关系,并进行了对比分析。对加固方案的工作机制进行了模拟,分析了这些方案在处理故障时的系统异常输出时间等容错特性。计算表明,这些加固方案可以显著提高系统的可靠性,其中双机互备加固方案的可靠性最高。该研究对于指导高可靠性自驾仪设计时在容错效果与复杂度、成本等方面进行折中具有较大的参考意义。

关键词:自驾仪;控制解算器;硬件加固;容错设计;可靠性增长
中图分类号:V241.4 **文献标志码**:A **文章编号**:1001-2486(2015)05-097-07

Hardware reinforcement designs and reliability analysis of unmanned aerial vehicle autopilots

GUO Tianhao[1], *HOU Zhongxi*[1], *JIANG Jingfei*[2], *JIANG Hanqing*[1]
(1. College of Aerospace Sciences and Engineering, National University of Defense Technology, Changsha 410073, China;
2. College of Computer, National University of Defense Technology, Changsha 410073, China)

Abstract: The autopilot is the crucial device for a unmanned aerial vehicle to implement autonomous flights and missions. Most of the existing commercial autopilots have no hardware reinforcement, which will lead to a risk in carrying out some significant tasks. The analysis reveals that the control resolver is the module which performs the greatest impact on the security and the reliability in the composing of an autopilot. With the increasing fault-tolerance requirements, 4 reinforcements were respectively designed, namely, the single resolver reset reinforcement, the dual resolver hot backup reinforcement, and the dual host systems switched by hardware and software. Several simple devices such as repositors, counters, inverters, selectors, and additional codes inside the resolvers were used to build the reinforcements. The reliabilities varying with time of the reinforcements were emphatically studied and comparatively analyzed. With the simulation of the working mechanisms, the fault-tolerance performances, such as the abnormal output durations, of the reinforcements in fault treatments were analyzed. The calculations show that all the reinforcements can obviously enhance the reliability of the autopilot, of which the dual host systems increase the most. This research provides a meaningful direction to the tradeoff of the fault-tolerance performance, complexity, and cost in high reliability autopilot designs.

Key words: autopilot; control resolver; hardware reinforcement; fault-tolerance design; reliability enhancement

无人机(Unmanned Aerial Vehicle, UAV)是一种由无线电遥控设备或自身程序控制装置操纵的无人驾驶飞行器[1]。自主性是无人机系统区别于有人驾驶飞机最重要的技术特征和发展趋势[2]。自驾仪是无人机实现自主飞行控制及自主完成各项任务的核心器件,设计安全可靠的无人机自驾仪具有十分重要的现实意义[3]。

无人机自驾仪通常由传感器组、控制解算器和执行机构三部分组成。传感器组用于采集无人机的速度、加速度、姿态、位置等状态信息。控制解算器由可编程芯片和内部的控制程序组成,主要用于根据无人机状态信息和预先设定好的控制算法,实时解算出各控制面需要执行的操纵量,以及与地面设备进行通信。无人机的自主性主要通过可编程芯片内部的程序来实现。执行机构用于对各控制面进行操纵。

* **收稿日期**:2014-11-10
基金项目:国家863计划资助项目(2014AA7052002)
作者简介:郭天豪(1989—),男,陕西汉中人,博士研究生,E-mail: upspark@qq.com;
侯中喜(通信作者),男,教授,博士,博士生导师,E-mail:hzx@nudt.edu.cn

相对于传感器组和执行机构,控制解算器内部结构更为复杂,并且运行着控制程序,其出错的可能性也更大。一旦控制解算器出现故障,没有容错处理的无人机将立即失控且无法和地面进行通信,有极大的概率坠毁。由于器件和内部程序等多方面原因,控制解算器出现故障总是难以避免[4-5]。对自驾仪的容错设计分为软件加固和硬件加固两种。通常的容错控制系统研究主要针对前者,通过优化控制解算器的内部程序,避免和处理一些程序级的故障和少部分有冗余信息的传感器故障[6-7]。现有的无人机商用自驾仪大多没有进行硬件加固,一方面降低复杂性及能耗,另一方面无人机在一个飞行架次之内各器件出错的概率较小,并且造价相对较低,发生故障产生的损失不大。然而,无人机有时会执行一些重大的任务或装有昂贵的机载设备,对可靠性和安全性的要求远高于平常。此时有必要对无人机自驾仪进行硬件加固,以此提高无人机的可靠性以及遇到故障时的生存概率[8]。

根据逐渐提高的可靠性要求,针对控制解算器硬件,即可编程芯片,以常用的数字信号处理器(Digital Signal Processor, DSP)为例,设计了不同的无人机自驾仪硬件加固方案,对其工作机制进行了模拟分析,重点对其可靠性进行了分析和比较。

1 加固硬件基础

1.1 所用的主要器件

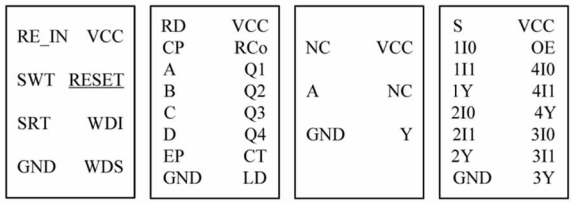
1)可编程芯片。采用 TMS320F28335 浮点 DSP 控制器,可内置程序、拥有丰富的通用输入/输出接口(General Purpose Input Output, GPIO)的数字处理芯片。

2)复位器。采用 MAX6746 芯片,带有看门狗定时器,可产生直接复位信号的多功能复位器。其接口如图 1(a)所示,SWT 端进行定时器的启动及阈值设置,WDI 端进行计时器的清零,当计时器达到阈值时,RESET 端会产生一个持续 300ms 的复位信号。

3)计数器。采用 74161 计数器,其接口如图 1(b)所示。Qi(i=1,2,3,4)为输出端,启动时全为逻辑“0”。CT 为使能端,为“1”时,进行正常计数,为“0”时,停止计数;CP 为时钟端,正常计数时,每接收到一个上升沿,Q1 进行一次翻转;每当 Qi 从“1”变为“0”时,Q(i+1)进行一次翻转。

4)反相门。采用 NLU1G04 单通道非门。其接口如图 1(c)所示,A 为输入端,Y 为输出端。当 A 为“0”时,Y 为“1”;反之 Y 为“0”。

5)选择器。采用 CD74HC257 四路 2 选 1 选择器。其接口如图 1(d)所示,S 为公共选择端,iI0 与 iI1 为输入端,iY 为输出端(i=1,2,3,4)。当 S 为“0”时,iY 等于 iI0,当 S 为“1”时,iY 等于 iI1。



(a)复位器 (b)计数器 (c)反相门 (d)选择器
(a) Repositor (b) Counter (c) Inverter (d) Selector

图 1 加固所用主要器件

Fig. 1 The main devices used in the reinforcements

1.2 器件的可靠性

评价系统能否可靠工作有众多指标,如可用度、可靠性、平均无故障时间、平均故障间隔时间、瞬时故障率等[8-9]。可靠性是指系统在某时间段内没有发生故障的概率。对于一旦发生故障会产生严重损失的系统,用可靠性作为评价指标更为合适[8]。

对于电子器件,在远小于其寿命的一个时间段内,通常认为瞬时故障率为常值。

设未经加固的 DSP 的瞬时故障率为 λ,可靠性为 $R_0(t)$。根据定义:

$R_0(t)=P(\forall\tau\in(0,t)$, DSP 在 τ 刻正常工作)

则 DSP 恰好在 t 时刻发生故障的概率为

$$f_0(t)=R_0(t)\lambda \tag{1}$$

DSP 在$(0,t)$时间段发生故障的概率为

$$F_0(t)=1-R_0(t) \tag{2}$$

且有

$$F_0(t)=\int_0^t f_0(\tau)\mathrm{d}\tau \tag{3}$$

将式(1)~(3)合并可以解得

$$R_0(t)=\mathrm{e}^{-\lambda t} \tag{4}$$

文中所用的复位器、计数器、反相门和选择器为简单逻辑硬件,其可靠性通常远高于 DSP 芯片,因而忽略这些器件出错的情形。

1.3 模拟验证方式

在 MATLAB 的 Simulink 仿真环境中,搭建自定义函数模块模拟各器件的功能,针对一路需要 DSP 处理的信号进行模拟。模拟中设定 DSP 的输入信号为 $x(t)=\sin(\pi t)$,输出信号为

$$y_0(t)=\begin{cases}2x(t)+1, & \text{DSP 正常工作;}\\ -1, & \text{DSP 发生故障;}\\ 0, & \text{DSP 正在初始化。}\end{cases}$$

模拟的目的是为了验证各加固方案的可用性以及其特点,在模拟验证中暂不考虑 DSP 启动或重启失败的状况。

给 DSP 在 $t=1$s 注入一次故障,模拟输出结果如图 2 所示。图中实线表示 DSP 实际输出数据,虚线表示 DSP 正常工作时的输出数据(期望输出数据)。

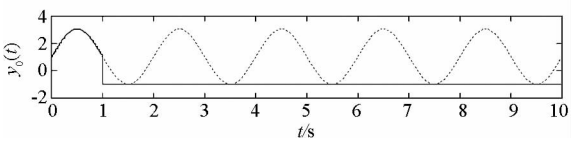


图 2　单 DSP 故障模拟输出

Fig. 2　The output with the DSP fault

2　加固方案设计

2.1　单机复位加固方案

2.1.1　加固方案

设计思路:当 DSP 出现故障时,用复位器对其进行重启。方案如图 3 所示。

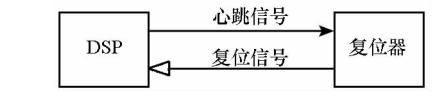


图 3　单机复位加固方案

Fig. 3　The single resolver reset reinforcement

在自驾仪上电时,DSP 会进行初始化,通过一个 GPIO 端口,对复位器进行设置,使定时器启动并设置阈值为 30ms。

在 DSP 内部添加一小段程序,使其每过 20ms(自驾仪控制周期)产生一个心跳信号,通过另一个 GPIO 端口,使得复位器内部的看门狗定时器清零并重新计时。

当 DSP 出现故障时,无法提供心跳信号,看门狗定时器会达到设定的阈值,复位器就会对 DSP 进行重启。

2.1.2　可靠性

故障发生后,复位器几乎立即对 DSP 进行重启。电子器件的故障有可能是由于过热造成,而这种重启发生时 DSP 仍然处于高温,因此有一定的失败率。称这样的重启方式为热重启,设其使系统恢复正常的概率为 P_R。

设该加固方案的可靠性为 $R_1(t)$,则系统恰好在 t 时刻发生故障的概率为

$$f_1(t)=R_1(t)\lambda(1-P_R) \tag{5}$$

系统在$(0,t)$时间段发生故障的概率为

$$F_1(t)=1-R_1(t)=\int_0^t f_1(\tau)\mathrm{d}\tau \tag{6}$$

合并以上两式可以解得

$$R_1(t)=\mathrm{e}^{-\lambda(1-P_R)t} \tag{7}$$

对比式(4)和式(7)可见,该加固方案的工作机理相当于降低了 DSP 的瞬间故障率,即在每一瞬间,系统发生故障的条件变为 DSP 发生故障且重启失败。

2.1.3　模拟验证

给 DSP 在 $t=1$s,$t=6$s 分别注入一次故障,系统输出结果如图 4 所示。

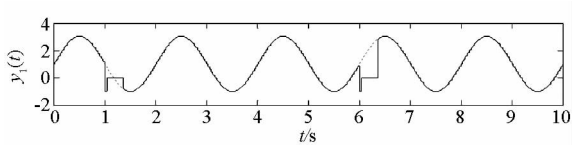


图 4　单机复位加固模拟输出

Fig. 4　The output of the single resolver reset reinforcement

由图 4 可见,当 DSP 发生故障后,输出异常值。30ms 后 DSP 接收到复位信号并持续 300ms,然后重启并需要 100ms 进行初始化,这段时间输出为 0。初始化完成后,DSP 恢复正常,输出正常信号。

该方案有两个不可避免的问题:①DSP 发生故障后,需要 430ms 才可能恢复正常,这对于自身具有良好稳定性的无人机通常是可以接受的,但对于高机动性无人机则有很大风险;②热重启有一定的失败率。为了增强克服以上问题的能力,设计了双机热备加固方案。

2.2　双机热备加固方案

2.2.1　加固方案

设计思路:为原系统 DSP(记为 DSPA)设置一个热备份(记为 DSPB)。二者同时接收各路数据并进行输出解算。当 DSPA 正常工作时,选择 DSPA 的输出数据;当 DSPA 发生故障时,对其进行一次复位,如果复位不成功,或者 DSPA 再次发生故障,则选择 DSPB 的输出数据。由于 DSPB 在作为备份时也是加电工作的,因而这种备份方式称为热备份。

在双机备份系统中,每 1 路 DSP 的输入信号都需要同时引入 DSPA 和 DSPB 中;每 1 路 DSP 的输出信号都需要引入选择器,根据两个 DSP 故障情况,选择其中 1 个输出作为系统的输出信号。方案如图 5 所示。

在自驾仪上电时,DSPA 会进行初始化,并对复位器进行设置。计数器初始化,Q2 为“0”,因此选择器的 S 端为“0”,输出来自 DSPA 的数据。

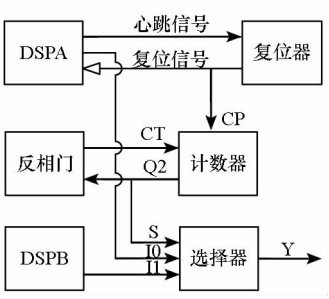


图 5 双机热备加固方案

Fig. 5 The dual resolver hot backup reinforcement

当 DSPA 出现故障时,无法提供心跳信号,复位器会对 DSPA 进行复位,同时该复位信号被计数器接收,使得 Q1 为“1”。如果复位没有成功,或复位成功后再次故障,复位器会再次发出复位信号,使得 Q2 为“1”,反相门输出“0”给计数器的使能端,令其停止计数,始终保持 Q2 为“1”,选择器 S 端为“1”,输出来自 DSPB 的数据。

2.2.2 可靠性

设该加固方案的可靠性为 $R_2(t)$。系统恰好在 t 时刻出现故障有以下几种情形:

1)DSPA 恰好在 t 时刻发生故障且复位失败,DSPB 在$(0,t)$时间段发生故障,其概率为:

$$f_{21}(t) = R_0(t)\lambda \cdot (1-P_R)F_0(t) = (1-P_R)\lambda e^{-\lambda t}(1-e^{-\lambda t}) \quad (8)$$

2)DSPA 在$(0,t)$时间段仅发生一次故障且复位成功,在 t 时刻又发生故障,DSPB 在$(0,t)$时间段发生故障,其概率为:

$$f_{22}(t) = \int_0^t R_0(\tau)\lambda P_R R_0(t-\tau)\mathrm{d}\tau \cdot \lambda F_0(t) = P_R\lambda^2 t e^{-\lambda t}(1-e^{-\lambda t}) \quad (9)$$

3)DSPA 在$(0,t)$时间段发生过故障且第一次复位失败,DSPB 恰好在 t 时刻发生故障,其概率为:

$$f_{23}(t) = F_0(t)(1-P_R) \cdot R_0(t)\lambda = (1-P_R)\lambda e^{-\lambda t}(1-e^{-\lambda t}) \quad (10)$$

4)DSPA 在$(0,t)$时间段发生多于一次故障且第一次复位成功,DSPB 恰好在 t 时刻发生故障,其概率为:

$$f_{24}(t) = \int_0^t R_0(\tau)\lambda P_R F_0(t-\tau)\mathrm{d}\tau \cdot R_0(t)\lambda = P_R\lambda e^{-\lambda t}(1-e^{-\lambda t}) - P_R\lambda^2 t e^{-2\lambda t} \quad (11)$$

因此,系统恰好在 t 时刻出现故障的概率为:

$$f_2(t) = f_{21}(t) + f_{22}(t) + f_{23}(t) + f_{24}(t) = (2 - P_R + P_R\lambda t)\lambda e^{-\lambda t} + (P_R - 2 - 2P_R\lambda t)\lambda e^{-2\lambda t} \quad (12)$$

系统在$(0,t)$时间段发生故障的概率为

$$F_2(t) = 1 - R_2(t) = \int_0^t f_2(\tau)\mathrm{d}\tau \quad (13)$$

合并以上两式可解得

$$R_2(t) = (2 + P_R\lambda t)e^{-\lambda t} - (1 + P_R\lambda t)e^{-2\lambda t} \quad (14)$$

2.2.3 模拟验证

给 DSPA 在 $t = 1\mathrm{s}, t = 6\mathrm{s}$ 分别注入一次故障,给 DSPB 在 $t = 8\mathrm{s}$ 注入一次故障。模拟结果如图 6 所示。图中 $y_A(t)$与 $y_B(t)$分别为来自 DSPA 与 DSPB 的输出数据,$y_2(t)$为系统输出数据。

当 DSPA 第一次出现故障且成功重启前后,系统仍然选择 DSPA 的数据作为输出,在其重启并初始化过程中,系统输出 0。当 DSPA 第二次发生故障后,系统选择工作正常的 DSPB 的数据作为输出,立即恢复正常输出。当系统已经启用 DSPB 的数据而 DSPB 发生故障时,由于没有进一步的容错措施,系统崩溃。

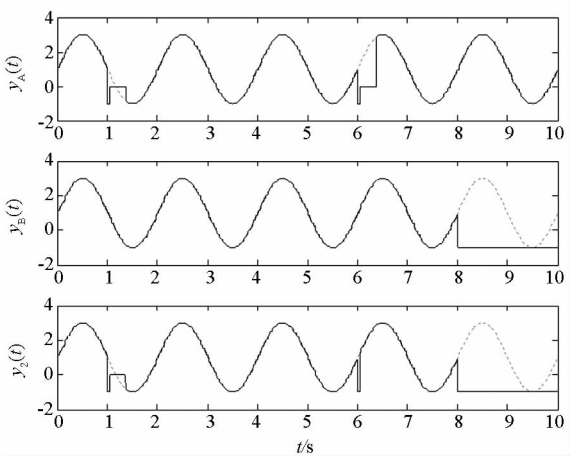


图 6 双机热备加固模拟输出

Fig. 6 The output of the dual resolver hot backup reinforcement

考虑到电子系统故障很大一部分是由过热引起,当系统启用 DSPB 的数据后,如果将发生故障的 DSPA 冷却一段时间然后再重启,则其有相当大的概率恢复工作,将其作为 DSPB 的备份可以很好地提高系统可靠性。基于这一想法,设计了双机互备加固方案。

2.3 硬件切换双机互备加固方案

2.3.1 加固方案

设计思路:为 DSP 设置双机互备系统,当 DSPA 故障时,选择 DSPB 的输出,同时将 DSPA 冷却作为备份;之后如果 DSPB 发生故障,重新启动 DSPA 并选择其输出,同时将 DSPB 冷却作为备份。这样的备份方式称为冷备份。方案如图 7 所示。

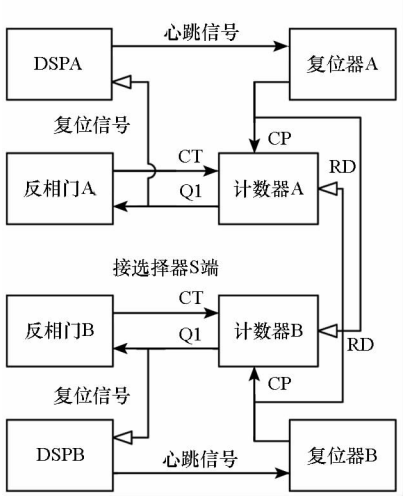


图 7　硬件切换双机互备加固方案

Fig. 7　The dual host system switched by hardware

在自驾仪上电时,计数器初始化使 Q1 为“0”,因此选择器(图中未画出)的 S 端为“0”,输出来自 DSPA 的数据。

当 DSPA 故障时,复位器 A 发出的复位信号使计数器 A 的 Q1 变为“1”,经过反相门引到使能端后,计数器 A 停止计数,保持 Q1 始终为“1”。Q1 引到 DSPA 的复位端使其保持冷却,同时引到选择器的 S 端使系统输出来自 DSPB 的数据。可见,这里的计数器实质上是起到了保持器的功能。

此后,如果 DSPB 也发生故障,复位器 B 发出的复位信号将计数器 A 清零,Q1 重置为“0”,则 DSPA 重启,同时选择器的 S 端为“0”,输出来自 DSPA 的数据。

2.3.2　可靠性

在故障发生后,复位器对 DSP 进行冷却一段时间然后重启,称这样的重启方式为冷重启。设冷重启的成功率为 P_C。

设该加固方案的可靠性为 $R_3(t)$。系统恰好在 t 时刻出现故障有以下几种情形:

1) DSPA 恰好在 t 时刻发生故障,DSPB 在 $(0,t)$ 时间段发生故障,冷却一段时间后在 t 时刻重启失败。其概率为

$$f_{31}(t) = R_0(t)\lambda \cdot F_0(t)(1-P_C) = (1-P_C)\lambda e^{-\lambda t}(1-e^{-\lambda t}) \quad (15)$$

2) DSPA 在 $(0,t)$ 时间段发生过故障并顺利切换到 DSPB,然后系统进入这样一种稳定模式:作为备份的 DSP 都处于故障并等待冷却重启。其恰好在 t 时刻发生故障的概率为

$$f_{32}(t) = \int_0^t R_0^2(\tau)\lambda \cdot R_C(t-\tau)\mathrm{d}\tau \cdot \lambda(1-P_C) \quad (16)$$

其中,上述稳定模式与单机复位方案类似,相当于将系统的瞬间故障率降为 $\lambda(1-P_C)$,其可靠性为

$$R_C(t) = e^{-\lambda(1-P_C)t} \quad (17)$$

将式(17)代入式(16)可得

$$f_{32}(t) = \frac{1-P_C}{1+P_C}\lambda\left[e^{-\lambda(1-P_C)t} - e^{-2\lambda t}\right] \quad (18)$$

系统恰好在 t 时刻出现故障的概率为

$$f_3(t) = f_{31}(t) + f_{32}(t) \quad (19)$$

系统在 $(0,t)$ 时间段发生故障的概率为

$$F_3(t) = 1 - R_3(t) = \int_0^t f_3(\tau)\mathrm{d}\tau \quad (20)$$

合并式(15)、式(18)~(20)可以解得

$$R_3(t) = \frac{P_C}{2} + (1-P_C)e^{-\lambda t} + \frac{1}{1+P_C}e^{-\lambda(1-P_C)t} + \frac{(P_C^2+P_C-2)}{2(1+P_C)}e^{-2\lambda t} \quad (21)$$

2.3.3　模拟验证

给 DSPA 在 $t=1$s,$t=6$s 分别注入一次故障,给 DSPB 在 $t=3$s,$t=8$s 分别注入一次故障。系统输出结果如图 8 所示。

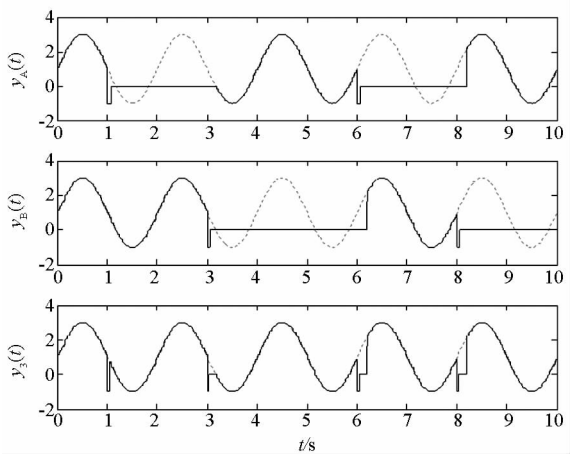


图 8　硬件切换双机互备加固模拟输出

Fig. 8　The output of the dual host system switched by hardware

可见,自驾仪上电时两个主备 DSP 均输出正常信号,当 DSPA 第一次故障时,系统输出切换到 DSPB,由于此时 DSPB 处于正常工作状态,因此一经切换系统立即输出正常信号。

此后系统对备份 DSP 的复位信号一直持续,使其冷却不进行运算。主 DSP 故障时,备份 DSP 重启并初始化,而此时系统输出已经切换到备份 DSP,因此初始化完成前系统输出为 0。

如果在此基础上,使备份 DSP 不等主 DSP 发生故障,而是冷却一段时间就自动重启,则在发生故障时系统可以立即输出正常值,达到最佳的加

固效果。然而,这一功能用简单硬件实现起来较为复杂,考虑到可以在 DSP 内部加一小段程序来实现,因而设计了软件切换双机互备加固方案。

2.4 软件切换双机互备加固方案

2.4.1 加固方案

设计思路:为 DSP 设置双机互备,当 DSPA 发生故障时,选择 DSPB 的输出,同时将 DSPA 冷却,一段时间后自动重启,但仍使用 DSPB 的数据,直到其发生故障再切换到 DSPA。设计方案如图 9 所示。

两个 DSP 芯片都可以监测对方的心跳信号,并通过复位电路(图中用黑色圆点表示)相互重启。复位电路由电阻、电容、三极管等简单元件组成,主要起到提供稳定复位电压的作用。具体切换的逻辑通过 DSP 中的程序实现。

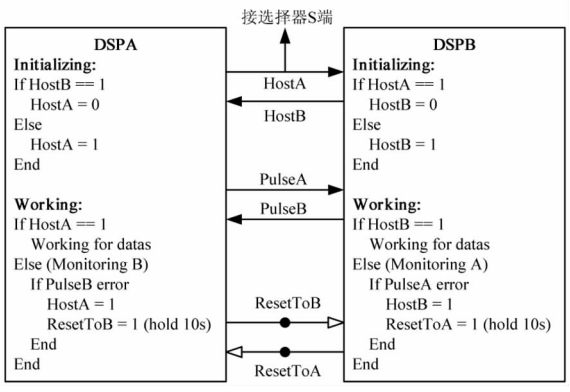


图 9 软件切换双机互备方案

Fig. 9 The dual host system switched by software

自驾仪上电时,DSPA 先启动,作为主机,DSPB 稍后启动,作为备机。DSP 在启动时,首先检测对方是否为主机:如果不是,则自己作为主机,进行正常驱动解算并输出;如果是,则自己作为备份,检测主机的心跳信号,如果发现主机故障,则给主机发出长度为 10s 的复位信号(即将主机冷却 10s 然后启动),同时自己切换为主机。

将 DSPA 是否为主机的信号接到选择器的 S 端。DSPA 为主机时,输出来自 DSPA 的信号;否则输出来自 DSPB 的信号。

由于本方案和硬件切换双机互备加固方案的切换流程是相同的,且都是冷重启,因而二者的可靠性相同。

2.4.2 模拟验证

为了较明晰地看到发生故障时的数据细节,模拟总时长不宜太大,因而在模拟验证中,将方案中的冷却 10s 减为冷却 0.5s。给 DSPA 在 $t=1$s,$t=6$s 分别注入一次故障,给 DSPB 在 $t=3$s,$t=8$s 分别注入一次故障。系统输出结果如图 10 所示。

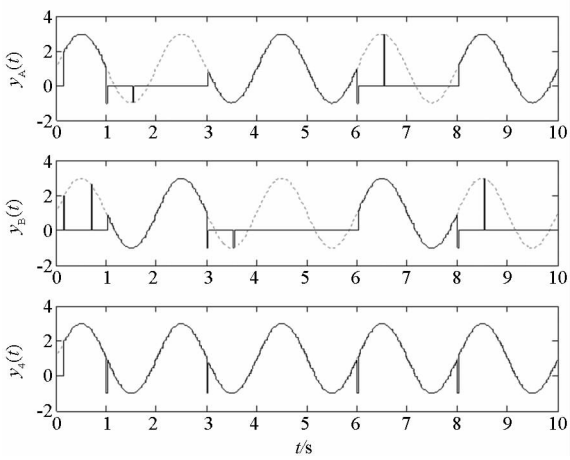


图 10 软件切换双机互备方案模拟输出

Fig. 10 The output of the dual host system switched by software

可见,自驾仪上电后 DSPA 为主,系统选择其数据进行输出。DSPB 作为备份,监测 DSPA 并输出 0。当 DSPA 发生故障后,DSPB 给 DSPA 发出复位信号并声明自己为主。DSPA 被冷却一段时间,期间不进行运算。之后进行初始化,初始化成功时会输出 1 帧解算信号,同时检测到 DSPB 为主后将自己作为备份。

通过模拟验证可以看出,系统在故障后切换时备份已经初始化完毕,故系统的非正常输出时间要更短,因而容错效果最优。

但应当指出,虽然软件切换双机互备方案在容错效果和硬件成本等方面要优于硬件切换,但是增加了原 DSP 的工作负荷以及程序出现 BUG 的风险。

3 加固方案可靠性比较

设置 $\lambda=2\times10^{-5}$/s,$P_R=0.8$,$P_C=0.95$,模拟时长为 15h,图 11 显示了各加固方案的可靠性

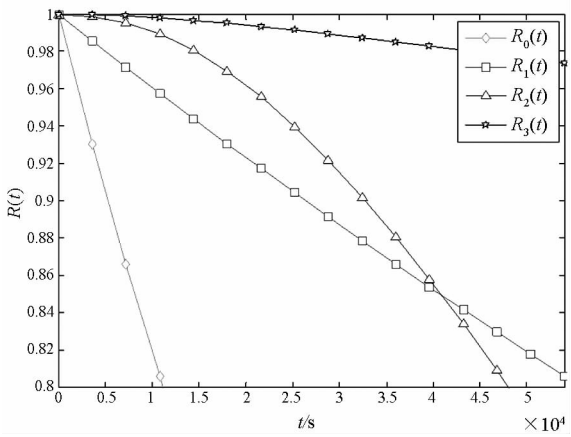


图 11 各加固方案可靠性对比图

Fig. 11 The reliabilities of the reinforcements

$R(t)$随时间的变化。

由图 11 可以看出,加固后的系统可靠性明显大于原系统;双机互备方案的可靠性最高;双机热备方案的可靠性在仿真前期大于单机复位方案,超过一段时间(该组参数下为 11.4h)后,其可靠性会低于单机复位方案,其原因是切换到备份 DSP 后,系统没有进一步的容错措施。

4　结论

根据逐步提高的加固要求,先后设计了四个自驾仪硬件加固方案,推导了这些方案的可靠性,并研究了这些方案在处理故障时的一些特点。通过理论推导与模拟分析的对比研究,得出以下结论:

1)在所设计的四个加固方案中,单机复位方案的复杂性与成本最低,虽然容错效果低于其他方案,但也能大幅提高系统的可靠性。

2)在所设计的四个加固方案中,双机互备系统的可靠性最高,其中软件切换方案处理故障时的系统异常输出时间最短。

本文对各加固方案的评价主要基于理论上的可靠性增长及处理故障时的系统异常输出时间。这些方案在实际工程应用时,还需要进行相应的供电电路设计、电路板布局设计。本文研究可以作为对无人机自驾仪进行硬件加固的参考。在具体选用哪种方案时,应当根据控制解算器工作负荷以及系统对可靠性、复杂度与成本的要求综合考虑。

参考文献(References)

[1] Department of Defense. Unmanned systems roadmap 2007 – 2032[R]. USA;Washington D. C., 2007.

[2] 朱华勇,牛轶峰,沈林成,等. 无人机系统自主控制技术研究现状与发展趋势[J]. 国防科技大学学报, 2010, 32(3): 115 – 120.
ZHU Huayong, NIU Yifeng, SHEN Lincheng, et al. State of the art and trends of autonomous control of UAV systems[J]. Journal of National University of Defense Technology, 2010, 32(3): 115 – 120. (in Chinese)

[3] Zugaj M, Narkiewicz J. Autopilot for reconfigurable flight control system[J]. Journal of Aerospace Engineering, 2009, 22(1):78 – 84.

[4] Bentley R M. Validating the pentium 4 microprocessor[C]// Proceedings of the International Conference on Dependable Systems and Networks, 2001:493 – 498.

[5] Zielger J F, Puchner H. SER-history, trends and challenges[R]. Cypress Semiconductor Corporation, 2004.

[6] DeLima P G, Yen G G. Tuning of fault tolerant control design parameters[J]. ISA Transactions, 2008, 47(1): 127 – 142.

[7] Goloubeva O, Rebaudengo M, Reorda M S, et al. Software implemented hardware fault tolerance CRC – TR 00 – 9[R]. USA: Center for Reliable Computing, 2000.

[8] Sorin D. Fault tolerant computer architecture[M]. USA: Morgan & Claypool Publishers, 2009.

[9] Mukherjee S. Architecture design for soft errors[M]. USA: Morgan Kaufmann Publishers, 2008.