

面向航电计算平台的多态动态故障树分析方法

孙东旭, 杨媛媛, 王红春, 王世奎, 贾世伟

(中航工业 西安航空计算技术研究所, 陕西 西安 710065)

摘 要: 针对航电计算平台的多态性、动态性的系统特点和不同计算性能的可靠度分析需求, 在传统动态故障树分析方法的基础上提出了支持多态性分析的串行门、并行门、条件门, 多态冷备件门, 设计了一种多态动态故障树分析方法. 采用该方法构建了一种典型架构航电计算平台的性能多态动态故障树, 基于蒙特卡洛仿真对该多态动态故障树进行了求解. 该方法可对航电计算平台不同性能要求下的可靠度进行定量分析, 为航电计算平台的可靠性设计提供理论数据支持.

关键词: 多态动态故障树; 性能可靠度; 蒙特卡洛仿真; 航电计算平台

中图分类号: TB114. 3

文献标识码: A

文章编号: 1000—7180(2017)05—0012—05

Multi-state Dynamic Fault Tree Analysis Method for Avionics Computing Platform

SUN Dong-xu, YANG Yuan-yuan, WANG Hong-chun, WANG Shi-Kui, JIA Shi-wei

(AVIC Computing Technique Research Institute, Xi'an 710065, China)

Abstract: In order to assess the performance reliability of dynamic and multi-state avionics computing platform, “serial gate”, “parallel gate”, “condition gate”, “multi-state cold spare gate” are proposed and a multi-state dynamic fault tree analysis method is designed for multi-state system analysis. A multi-state dynamic fault tree of representative structure avionics computing platform is constructed using the dynamic fault tree analysis method and calculated by Monte Carlo simulation. The multi-state dynamic fault tree analysis method can evaluate performance reliability of avionics computing platform under different performance requirements, and can provide theoretical data for reliability design of avionics computing platform.

Key words: multi-state dynamic fault tree; performance reliability; monte carlo simulation; avionics computing platform

1 引言

航电计算平台(ACP)是综合模块化航电系统的关键组成部分, 基于模块化、软硬件综合等方法给飞机提供了容错、灵活可配置的共享计算服务, 承担了整架飞机海量数据的计算任务^[1-2]. 由于 ACP 的计算性能对飞机功能实现和任务完成具有重大影响, 因此准确评估其计算性能的可靠性具有重要意义.

ACP 中存在热备份、冷备份、备件共用的动态容错逻辑关系以及计算资源与电源、网络的功能依

赖关系, 难以用静态故障树、FMEA 等静态方法^[3]进行准确分析. 为适应容错计算机可靠性分析需要, Dugan JB 等人在静态故障树的基础上增加了时序依赖、备件门等动态门, 提出了动态故障树分析方法^[4]. 近年来, 动态故障树在动态系统分析中得到了广泛应用^[5-7], 但是传统的动态故障树分析方法中的门仅支持二态变量的输入输出, 只能完成系统的正常/故障二态分析, 不能对多态系统中介于正常和故障之间的中间状态进行定量分析. 而 ACP 虽然由多个故障形式为正常/故障的二态模块组成, 但在不同的故障情况下 ACP 表现出多种工作状态并输出不

同的计算性能,是一种典型的二态组件多态系统^[8-9],因此不能简单地分析 ACP 正常/故障二态情况,而应对其具有多态性的计算性能的可靠度进行定量分析. 本文在传统动态故障树的基础上提出了串行门、并行门、条件门、多态冷备件门几个多态门,设计了一种多态动态故障树分析方法,对 ACP 不同计算性能的可靠度进行了分析.

2 典型航电计算平台架构及性能可靠度定义

一个典型的 ACP 组成架构如图 1 所示,其中通用计算子系统、数据计算子系统、信号计算子系统组成计算资源. 其中通用计算子系统(GCS)包含 5 块工作通用计算模块(GCM)和 1 块共用的 GCM 冷备件,数据计算子系统(DCS)包含 4 块数据计算模块(DCM)和 1 块共用的 DCM 冷备件,信号计算子系统(SCS)包含 4 块信号计算模块(SCM)和 1 块共用的 SCM 冷备件. ACP 采用两块热备份的交换机(SW)实现交换网络和 2 块热备份的电源模块(PM)实现电源网络.

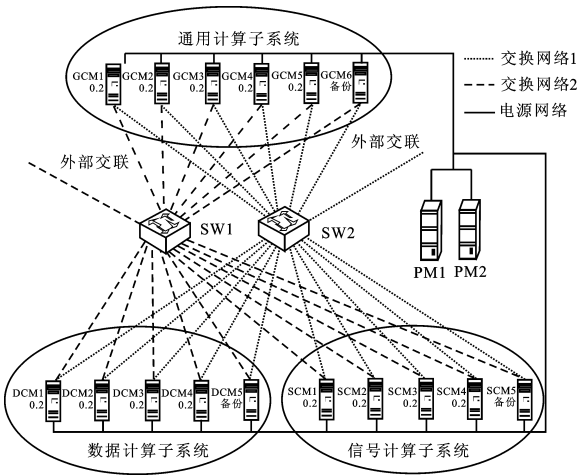


图 1 航电计算平台系统架构图

各个计算子系统组成模块并行计算,子系统计算性能为组成模块的总和;各个子系统之间串行计算,串行计算性能为各个子系统计算性能的最低值. 本文采用归一化的形式描述计算性能,单块 GCM 正常工作时性能为 0.2,单块 DCM、SCM 正常工作时性能为 0.25,当 GCM、DCM、SCM 故障或处于冷备份状态时性能为 0. SW1、SW2、PM1、PM2 仅有故障及正常两种状态,ACP 计算功能的实现依赖可用的交换网络和电源网络,当交换网络和电源网络可用时,ACP 计算性能与 GCS、DSC、SCS 串行计算性能一致;当交换网络或电源网络故障时,航电计

算平台计算性能为 0. 为便于描述,本文将性能可靠度 $R[a]$ 定义如下:

性能可靠度 $R[a]$ 为在规定的时间和规定的条件下,可实现计算性能 a 及以上计算性能的概率.

3 多态门定义

3.1 并行门

并行门用于分析输出为组成单元输出总和的系统,并行门适用于分析 ACP 中各个计算子系统中并行计算的组成关系,并行门的图示如图 2 所示.

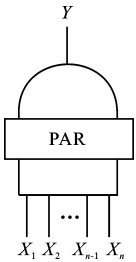


图 2 并行门

并行门含有一个连续型非负输出变量 Y 和 n 个连续型非负输入变量 $\{X_1, X_2, \dots, X_n\}$. 并行门的计算公式如式(1)所示,并行门输出变量 Y 等于 n 个输入变量 $\{X_1, X_2, \dots, X_n\}$ 之和.

$$Y = \sum_{i=1}^n X_i$$

(1)

3.2 串行门

串行门用于分析输出为组成单元输出值中最小值的系统,适用于分析 ACP 中各个子系统之间串行计算的组成关系,串行门的图示如图 3 所示.

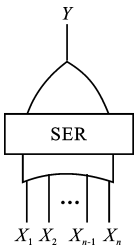


图 3 串行门

串行门含有一个连续型非负输出变量 Y 和 n 个连续型非负输入变量 $\{X_1, X_2, \dots, X_n\}$. 串行门的计算公式如式(2)所示,串行门输出变量 Y 等于 n 个输入变量 $\{X_1, X_2, \dots, X_n\}$ 中的最小值.

$$Y = \min_{1 \leq i \leq n} X_i$$

(2)

3.3 条件门

条件门用于分析二态条件对连续型输入具有开

关作用的系统,适用于分析 ACP 中计算资源对于网络和电源的依赖关系,条件门的图示如图 4 所示。

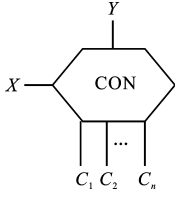


图 4 条件门

条件门包含一个连续型非负输出变量 Y 、一个连续型非负输入变量 X 和 n 个二态变量 $\{C_1, C_2, \dots, C_n\}$ 。条件门的计算公式如式(3)所示,当条件事件 $\{C_1, C_2, \dots, C_n\}$ 都不发生(等于 0)时,条件门的输出变量 Y 与输入变量 X 相同,当条件事件 $\{C_1, C_2, \dots, C_n\}$ 中任意事件发生(等于 1)时,输出变量 Y 为 0。

$$Y = \begin{cases} X, & \text{if } C_i = 0, i \in \{1, 2, \dots, n\} \\ 0, & \text{otherwise} \end{cases} \quad (3)$$

3.4 多态冷备件门

传统冷备件门中第一个输入刚开始即进入工作状态,其余输入进入储备状态且发生概率为 0;当上一个输入发生(等于 1),后一个输入进入工作状态;当所有输入发生,输出事件发生(等于 1)^[4]。传统冷备件门输入输出事件仅支持二态变量。多态冷备件门在传统冷备件门的基础上增加了多态特性使其适用多态系统的分析,其图示如图 5 所示。

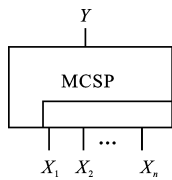


图 5 多态冷备件门

多态冷备件门包含一个连续型非负变量 Y 和 n 个非负连续型变量 $\{X_1, X_2, \dots, X_n\}$,多态冷备件门的计算公式如式(4)所示。第一个输入刚开始就进入工作状态,其余输入作为备件输入进入储备状态且发生概率为 0,输出变量 Y 与第一个输入变量 X_1 相同,当上一个输入 $X_{i-1}, i \in \{2, 3, \dots, n\}$ 失效(输入值变为 0),后一个输入 $X_i, i \in \{2, 3, \dots, n\}$ 替代上一个失效输入进入工作状态,输出变量 Y 转变为与 X_i 相同,当所有输入变量变为 0 后,输出变量 Y 为 0。在多个冷备件门共用一个备件输入时,仅当该储备输入处于储备状态时才可替代失效输入。

$$Y = \begin{cases} X_1, & \text{if } X_1 > 0 \\ X_i, & \text{if } \{X_1 = 0, X_2 = 0, \dots, X_{i-1} = 0, \\ & X_i > 0\}, i \in \{2, 3, \dots, n\} \\ 0, & \text{otherwise} \end{cases} \quad (4)$$

4 典型架构 ACP 性能多态动态故障树建模

4.1 构建性能多态动态故障树

在已定义的多态门的基础上构建图 1 所示的典型 ACP 的性能多态动态故障树如图 6 所示。子系统串行计算性能与交换网络故障、电源网络故障之间采用条件门连接,来表征 ACP 功能实现对交换网络和电源网络的依赖关系,当交换网络故障、电源网络故障均不发生时,ACP 计算性能输出与子系统串行计算性能一致,否则,ACP 计算性能输出为 0;GSC 计算性能、DCS 计算性能、SCS 计算性能采用串行门连接,表征子系统之间串行计算时的性能瓶颈特点。SW1 和 SW2 采用传统动态故障树中的热备份动态门连接,表征 SW1 和 SW2 同时工作,只有在 SW1 和 SW2 同时故障时,才会导致交换网络故障,ACP 启动时 SW1、SW2 均进入工作状态并具有一致的失效率。同理 PM1 和 PM2 也采用热备份动态门连接。

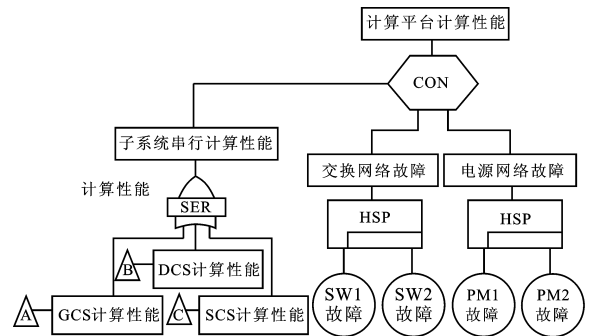


图 6 ACP 计算性能多态动态故障树

GCS 计算性能多态动态故障子树展开如图 7 所示,GCS 中各个 GCM 并行计算,GCS 的计算性能为所有工作 GCM 的性能总和,因此各个 GCM 采用并行门进行连接;同时 GCS 中具有冷备份和备件共用的容错逻辑关系,因此 5 个工作 GCM 与共用备件 GCM 同时采用多态冷备件门进行连接。当 ACP 启动时,GCM1-GCM5 进入工作状态,GCM6 进入贮备状态并且失效率为 0。当第一块 GCM 故障时,备件 GCM 进入工作状态并与工作 GCM 具有一致的失效率,GCS 计算性能维持原有输出;后续出现的故障 GCM 无可用备件,GCS 计算性能输出按每块故障模块 0.2 递减。

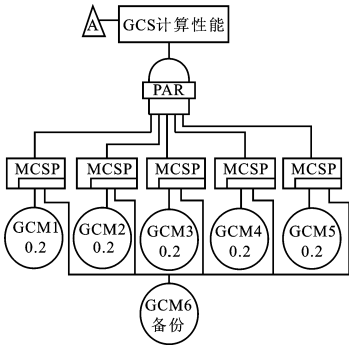


图 7 GCS 计算性能子树

参照通用 GCS 多态动态故障子树,分别建立 DCS 多态动态故障子树和 SCS 多态动态故障子树如图 8 和图 9 所示。

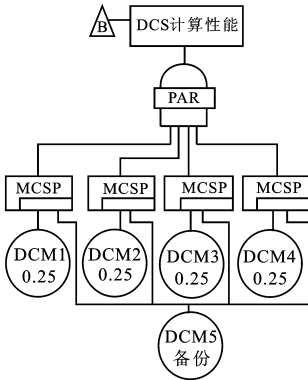


图 8 DCS 计算性能子树

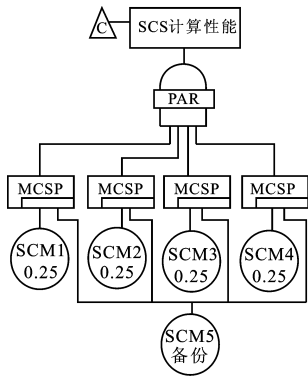


图 9 SCS 计算性能子树

4.2 仿真与计算

由于多态动态故障树具有复杂的多态性和动态性逻辑关系,难以采用马尔可夫链等解析方法进行计算。蒙特卡洛仿真是一种基于随机变量的统计试验或随机模拟方法,简单灵活并且易于编程实现,适合复杂系统的分析^[10]。本文将蒙特卡洛仿真应用于多态动态故障树计算中,采用仿真观测性能可靠度值来估计总体性能可靠度。

在仿真过程中,对于 ACP 启动即进入工作状态的模块,模块状态分为工作、失效两种状态,当模块故障分布随机抽样值小于规定的仿真系统时间,模块进入失效状态;而对于多个模块共用的冷备件,备件状态分为储备、工作、失效三种状态,冷备件仅在储备状态时替换失效模块并进入工作状态,而在工作状态和失效状态时不能对失效模块进行替换,以保证共用冷备件仅能使用一次。当冷备件进入工作状态时间与备件寿命随机抽样值相加小于规定的仿真系统时间,冷备件进入失效状态。在仿真时间结束时,根据各个模块的状态和各个门的公式计算 ACP 的性能。

以图 7 所示的 GCS 计算性能子树为例,设各个模块储备状态为 S_0 ,工作状态为 S_1 ,失效状态为 S_2 ,仿真系统时间 T_{sys} ,GCM 模块失效率为 λ ,单次蒙特卡洛仿真中 GCS 计算性能 P_{GCS} 计算流程如下图 10 所示。

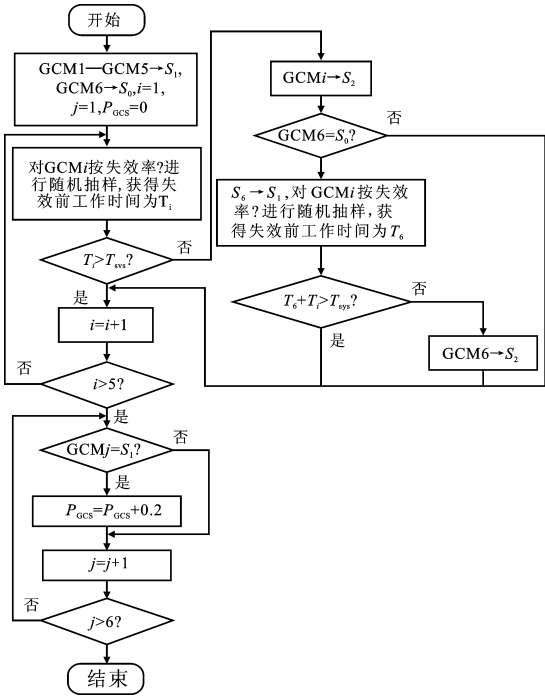


图 10 GCS 计算性能子树仿真流程

设蒙特卡洛仿真次数为 M 次,ACP 性能要求为 a 时的性能可靠度 $R[a]$ 计算公式如式(5)所示,其中 $P[N]$ 为在第 N 轮的仿真中根据各个门的规则计算出的 ACP 性能, $R[a]$ 为在 M 次的仿真中 ACP 性能大于等于规定值 a 的比例。

$$R[a] = \sum_{N=1}^M \frac{X[N]}{M}, X[N] = \begin{cases} 1, & \text{if } P[N] \geq a \\ 0, & \text{otherwise} \end{cases} \quad (5)$$

4.3 结果分析

仿真软件采用 MATLAB, 仿真次数设置为 1×10^5 次, 设 GCM 故障率为 0.01/h, DCM 故障率为 0.01/h, SCM 故障率为 0.015/h, SW 故障率为 0.015/h, PM 故障率为 0.02/h.

图 11 给出了 ACP 不同性能的可靠度随任务时间变化情况, 可见性能可靠度 $R[1.0]$ 、 $R[0.8]$ 随任务时间的增长呈现出较高的下降速度, 在 10h 时刻降至 0.8 以下, 而性能可靠度 $R[0.75]$ 、 $R[0.6]$ 、 $R[0.5]$ 下降速度较慢, 在 10h 时刻仍高于 0.9. 从图 10 可知, 在不同的性能要求、不同的任务时间, ACP 具有不同的性能可靠度; 此外, 随着任务时间的增长, ACP 可实现 0.8 以上的性能的性能可靠度下降较快. 因此, 进行计算任务规划时, 对于需 0.8 计算性能才能完成的计算任务, 需要规划较短的任务时间; 而对于需较长时间执行的计算任务, 应设法降低任务对计算性能的要求至 0.75 以下.

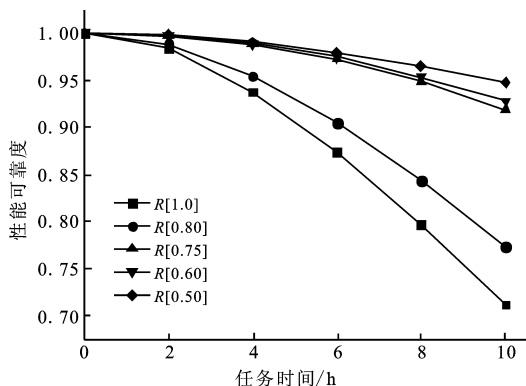


图 11 计算平台性能可靠度

本文对不同容错方案下 ACP 的不同性能的可靠度进行了比较. 图 12 为不同容错方案对 ACP 性能可靠度 $R[1.0]$ 的影响, 可看出 SCM、GCM 备件对 ACP 性能可靠度 $R[1.0]$ 影响最大, 在性能要求为 1.0 时 SCM、GCM 备件具有更高的重要程度. 图 13 为不同容错方案对 ACP 性能可靠度 $R[0.75]$ 的影响, 可看出 PM 备件少、SW 的减少对 ACP 的性能可靠度 $R[0.75]$ 影响更大, 在性能要求为 0.75 时, PM、SW 备件具有更高的重要程度. 由图 12、图 13 可知, 各个模块对 ACP 性能可靠度具有不同的影响并且在不同的计算性能要求下具有不同的重要程度, 在进行可靠性设计时候需要根据不同的计算性能要求优先改进重要程度更高的模块并采用合适的容错方案.

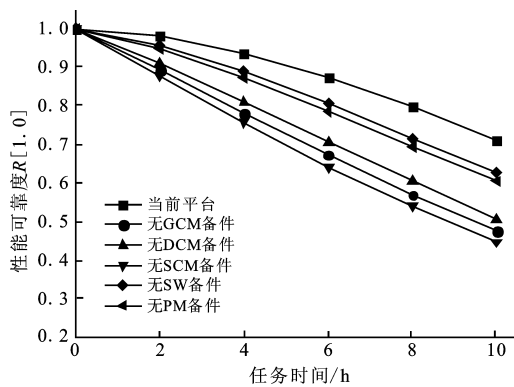


图 12 几种容错方案下 $R[1.0]$ 比较

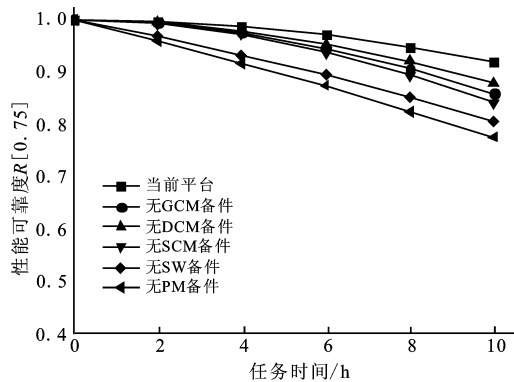


图 13 几种容错方案下 $R[0.75]$ 比较

5 结束语

相比仅能分析系统正常/故障情况的传统动态故障树, 多态动态故障树分析方法增加了并行门、串行门、条件门和多态冷备件门, 可对 ACP 具有多态性的计算性能的可靠度进行定量分析, 为 ACP 计算任务规划、可靠性设计优化等提供更详细的数据支持.

参考文献:

- [1] Roland Wolfig. 牛文生, 译. 综合化模块化航空电子系统的分布式平台[M]. 北京: 航空工业出版社, 2015.
- [2] Integrated Modular Avionics (IMA) development guidance and certification considerations [S]. Washington, D. C. USA, Radio Technical Commission for Aeronautics, Inc. 2005.
- [3] 曾声奎. 可靠性设计与分析[M]. 北京: 国防工业出版社, 2013.
- [4] Dugan J B, Bavuso S J, Boyd M A. Dynamic fault-tree models for fault-tolerant computer systems [J]. IEEE Transactions on Reliability, 1992, 41 (3): 363-377.

及 PLL 电路实现步进粗调,而通过 DDS 提供输出频率的小步进调节.

DDS 内插式频率合成器的 PLL 结构中,采用高 Q 值的窄带环路滤波器,可以对 DDS 输出信号中的大部分杂散信号进行有效抑制,如果从杂散抑制的角度来考虑,PLL 的环路带宽越窄,杂散落在通带内的概率就越小,杂散抑制效果越明显,合成器输出的频谱就越理想.因此,这种模式比较适合频点较少的窄频带系统.

4 结束语

DDS 与 PLL 混合频率合成技术以优势互补的形式改进了频率合成性能,弥补了单一模式存在的不足^[7].DDS 激励 PLL 的形式,实现了高频率分辨率,在保证宽带频率合成的同时,解决了频率小步进问题,在一定频率范围内,可以相对理想的改善频率合成器的近端杂散问题.而 DDS 以内插的方式引入 PLL,对杂散、谐波等抑制比较明显,但使用频带较窄.两种方法各自有其不同的特点和适用范围.根据频率合成的目的、要求,选择不同的混合模式,改善频率合成效果.

参考文献:

[1] 赵宏飞. 4.8GHz 宽带 DDS 锁相扫频源的研制[D]. 成都: 电子科技大学, 2002.

[2] Ulich L Rohde. Microwave and wireless synthesizer: theory and design [M]. New York: Wiley Interscience, 1997.

[3] 白居易. 直接数字频率合成[M]. 西安: 西安交通大学出版社, 2007.

[4] 侯卫国. 基于 DDS+PLL 的 S 波段小步进频率合成器的研究与设计[D]. 成都: 电子科技大学, 2010.

[5] 陈大海, 邓贤进, 张健. 宽带频率合成器设计及应用[J]. 电子测量与仪器学报, 2008, 22(1):94-98

[6] 王轶. 基于 DDS+PLL 技术的高性能频率源研究与实现[D]. 长沙: 国防科学技术大学, 2004.

[7] 高玉良. 现代频率合成与控制技术[M]. 北京: 航空工业出版社, 2002.

作者简介:

王 锋 男, (1980-), 博士, 讲师. 研究方向为测试技术及信号处理. E-mail: wangfeng1111@126. com.

刘鹏远 男, (1975-), 博士, 副教授. 研究方向为测试与仿真技术.

李 兵 男, (1982-), 博士, 副教授. 研究方向为测试技术及信号处理.

(上接第 16 页)

[5] 武文斌, 汪立新, 周小刚, 等. 基于改进的动态故障树的惯导系统安全性分析[J]. 航天控制, 2011, 29(5): 63-66.

[6] 熊小萍, 谭建成, 林湘宁. 基于动态故障树的变电站通信系统可靠性分析[J]. 中国电机工程学报, 2012, 32(34): 135-143.

[7] Li Xinkun, Huang Ning, Zheng Xiaoyan. Application based dynamic fault tree method for AFDX network [C] //Annual Reliability and Maintainability Symposium. Arizona, USA ,Tucson, AZ, IEEE, 2016.

[8] Anatoly Lisnianski Ilia Frenkel. Recent advances in system reliability [M]. London, Springer, 2012.

[9] Hoang Pham. Handbook of reliability engineering [M]. London: Springer, 2003.

[10] 曾畅, 方强, 吴军, 等. 蒙特卡洛模拟法在复杂系统可

靠性仿真中的应用研究[J]. 四川兵工学报, 2015, 36(9): 65-68.

作者简介:

孙东旭 男, (1987-), 硕士, 工程师. 研究方向为航电系统的五性技术. E-mail: sdx_fc@163. com.

杨媛媛 女, (1988-), 硕士, 工程师. 研究方向为机载通信网络.

王红春 男, (1977-), 博士, 研究员. 研究方向为计算机网络与通信.

王世奎 男, (1965-), 硕士, 研究员. 研究方向为计算机网络与通信.

贾世伟 男, (1987-), 硕士, 工程师. 研究方向为航电系统的五性技术.