引用格式:孙东旭,李键,武健.面向IMA平台的离散事件演化树仿真分析方法[J].电光与控制,2019,26(2):97-100. SUN D X, LI J, WU J. Simulation analysis method of discrete event evolution tree for IMA Platform[J]. Electronics Optics & Control, 2019, 26(2):97-100.

面向IMA平台的离散事件演化树仿真分析方法

孙东旭, 李 键, 武 健
(航空工业西安航空计算技术研究所,西安 710065)

摘 要: 为解决具有时序相关、功能依赖、多态性、部件数量多等特点的IMA平台在可靠性分析中的困难,提出了一种离散事件演化树仿真分析方法,通过将IMA平台运行过程中的随机故障事件建立成离散故障事件序列,从而驱动系统状态的不断演化,利用故障事件演化树分析离散故障事件对系统状态的影响,通过建立系统多状态集合和大样本观测评估IMA平台在不同时刻处于各个系统状态的概率。该离散事件演化树仿真分析方法可实现IMA平台可靠性多态定量分析,为设计提供理论数据依据。

关键词: IMA平台; 离散事件演化树; 可靠性分析; 仿真分析方法
中图分类号: V215.7 **文献标志码**: A **doi**:10.3969/j.issn.1671-637X.2019.02.021

Simulation Analysis Method of Discrete Event Evolution Tree for IMA Platform

SUN Dong-xu, LI Jian, WU Jian
(Computing Technique Research Institute, AVIC, Xi'an 710065, China)

Abstract: The IMA platform has such characteristics as time correlation, function dependence, multiple states and numerous parts. To solve the difficulty of the IMA platform in reliability analysis, a method for Discrete Event Evolution Tree (DEET) simulation analysis was proposed. In the running process of the IMA platform, the random failure event was transformed into a discrete failure event sequence, so as to drive the constant evolution of the system state. The evolution tree of the failure event was used to analyze the impact of the discrete failure event on the system state. Then, the multi-state sets and large sample observation were set up to evaluate the probability of the IMA platform being in different states at different time. The DEET method can quantitatively analyze the multi-state reliability of the IMA platform and serve as a theoretical data basis for further design.

Key words: IMA platform; discrete event evolution tree; reliability analysis; simulation analysis method

0 引言

综合模块化架构(IMA)是新型的航电系统架构,其通过业务与硬件分离的设计,基于重构的容错设计极大地提高了业务部署的灵活性和可靠性[1]。在IMA架构中,航电系统的大部分功能实现都需要依赖IMA平台来实现,因此定量地分析IMA平台的可靠性具有重要意义[2]。然而,IMA平台工作可靠性分析存在以下困难:1) IMA平台采用的基于重构的容错设计使得其状态和各个组成部件故障次序有关,而且故障演化过程中各个部件相互作用相互依赖,大量的时序相关、功能依赖动态关系[3]导致难以用精确的故障数学模型来描述[4],也难以用传统的RBD[5],FMEA[6]和FTA[7]等静态分析方法来分析;2) IMA平台是一种典型的多态性复杂系统[8],不但部分部件存在储备/工作/故障等多种状态,整个IMA平台更是存在不同业务处理能力和维修需求的多种状态,分析IMA平台的可靠性需要评估各个状态的状态概率,因此也不能用仅支持二态分析的动态方法,如DFT方法进行分析[9];3) IMA平台中部件数量多,内部交联关系复杂,采用Markov[10]链、SPN方法[11]等基于状态空间的分析方法时将会出现系统状态空间的组合爆炸问题,建模困难并且难以解析。

离散事件仿真(DES)技术可深入分析系统内部活动细节、建模能力强的优点使得其成为复杂系统可靠

收稿日期:2018-01-29 修回日期:2018-03-22
基金项目:航空科学基金(2014ZC31002)
作者简介:孙东旭(1987—),男,湖南邵阳人,硕士,工程师,研究方向为航电系统可靠性技术。

性分析的重要新方向，近年来在化学[12]、土木工程[13]、医疗[14]、核工业[15]等领域的可靠性分析中均有广泛的应用，但现有的 DES 方法仍然无法满足同时具有时序相关、功能依赖、多态性和部件数量多特点的 IMA 平台的可靠性分析。为解决 IMA 可靠性分析中的困难，本文基于 DES 的思想，提出了一种离散事件驱动演化树(DEET)仿真分析方法，实现了 IMA 平台可靠性多态定量分析。

1 典型的 IMA 组成架构

典型的 IMA 平台组成架构如图 1 所示，n 个通用处理模块(GPM)和 k 块 GPM 备件组成公共计算资源(CCR)，以上公共计算资源通过交换机(SW)提供的交换网络进行连接，任务管理器(TM)负责监控各个 GPM 的工作状态，并在 GPM 发生故障后将业务迁移至备份的 GPM 中进行 IMA 平台业务的重构，IMA 平台中随平台启动即进入工作状态的部件具有工作/失效两种状态，GPM 备件具有储备/工作/失效 3 种状态。

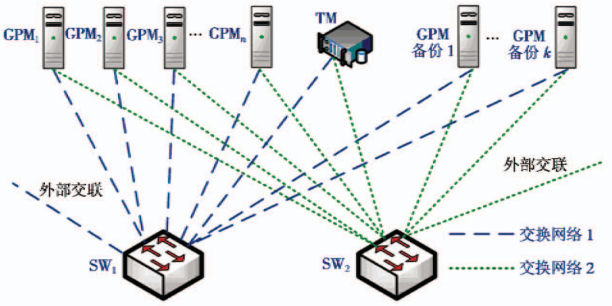

图 1 典型的 IMA 架构

Fig. 1 Typical IMA architecture

2 DEET 仿真分析方法

DEET 仿真分析方法通过将 IMA 平台运行过程中的随机故障事件建立成离散故障事件序列，驱动系统状态的不断演化，解决分析中的时序相关问题，并通过局部演化与全局信息共享结合的故障事件演化树解决分析中的功能依赖和状态空间复杂问题，通过建立 IMA 平台多状态集和通过大样本观测值评估系统在指定时刻处于各个状态的概率，解决分析中的多态性问题。

2.1 离散事件驱动

为解决时序相关方面的分析困难，DEET 方法首先将 IMA 平台中每个部件故障作为一个离散事件，并在每轮仿真中将所有在系统工作时间内发生的离散故障事件按故障发生时间先后排列成驱动事件序列；然后，驱动事件序列中的故障事件不断驱动故障事件演化树分析系统状态在故障事件发生后的更新结果，并在系统状态更新引发了新的故障事件(如备件从储备状态经过工作状态再进入故障状态的事件)时根据时间将新的故障事件插入驱动事件序列，DEET 方法的离散事件驱动仿真机制如图 2 所示。

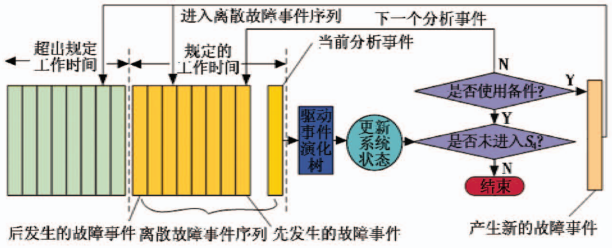

图 2 离散事件驱动仿真机制

Fig. 2 Simulation mechanism driven by the discrete event

DEET 方法在仿真过程中维护一个离散故障事件序列

$$E=\{e_1,e_2,\cdots,e_n \mid \max(t_{e1},t_{e2},\cdots,t_{en})\leqslant T_S\} \quad (1)$$

式中：E 为事件序列；t_{ei} 为序列中故障事件 e_i 发生的时刻；T_S 为指定的系统状态观测时刻。为观测系统运行到 T_S 时刻系统所处的状态，DEET 方法将 T_S 时刻前发生的故障事件放入驱动序列，将 T_S 时刻之后发生的故障事件丢弃。

故障事件 e_i 失效的时刻 t_{ei} 产生方法为

$$t_{ei}=g(f_i(t))+t_i \quad (2)$$

式中：$g(f_i(t))$ 为根据部件 i 的故障概率密度 $f_i(t)$ 进行随机抽样得到的故障发生前工作时间；t_i 为部件 i 开始工作的时刻，对于一开始就进入工作状态的只具备工作/失效 2 种状态的部件，$t_i=0$，而对于具备储备/工作/故障 3 种状态的部件，其 t_i 为所替换故障部件由储备状态进入工作状态的时刻。

2.2 故障事件演化树

IMA 平台在故障演化过程中存在相互依赖、相互影响的复杂关系，如当 GPM 发生故障时，IMA 的平台重构依赖 TM 正常工作和可用的备件，并且 IMA 平台中部件数量众多，导致穷举完整的状态空间和分析状态之间的转移难以实现。为解决以上困难，DEET 将部件发生故障后系统状态变化的过程构建为树形结构，使用当前系统状态和各个部件的储备/工作/失效状态信息作为全局信息，用于树形演化过程中分支判断条件；同时，根据局部演化过程中对全局信息的影响进行全局信息的更新，如 GPM 发生故障后将应用迁移到 GPM 备件，GPM 备件由储备状态进入工作状态，同时减少了剩余备件的数量。通过全局信息和局部演化相结合构建故障事件演化树，DEET 方法既可以详细建模故障演化过程中 IMA 各部件功能相互依赖、状态相互影响的过程，又可以大大降低分析过程中的状态空间大小。

为满足多态性分析的要求，在使用 DEET 方法时，根据分析的目的和颗粒度建立系统多状态集合，如表

1 为本文根据 IMA 平台可完成业务的能力以及对维修的需求，将 IMA 平台系统状态描述为 $\{S_1, S_2, S_3, S_4\}$ 4 状态集合。

表 1　IMA 平台 4 状态集合

Table 1　Four-state set of IMA platform

状态定义	含义
S_1	初始状态，不需要维修
S_2	能完成全部业务，需维修
S_3	能处理部分业务，需维修
S_4	终止态，全部功能丧失，需维修

典型 IMA 平台架构中 GPM 故障的故障事件演化树示例如图 3 所示，事件演化树根据更新前的系统状态进入不同的分支；然后，根据全局信息中 TM 的工作状态、剩余 GPM 备件的数量、剩余工作 GPM 的数量完成系统状态、备件数量等全局信息的更新，SW 故障和 TM 故障的演化树可参考图 3 建立。

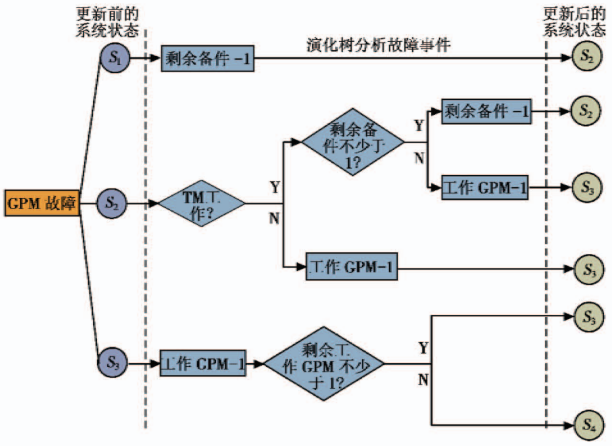

图 3　GPM 故障事件演化树

Fig. 3　Evolution tree of GPM failure event

2.3　状态概率计算

为计算 IMA 平台各个状态的状态概率，DEET 方法通过重复随机仿真试验采集大量的样本，通过统计样本数据中的状态概率估计总体的状态概率。DEET 方法仿真流程如图 4 所示，在每轮仿真前，指定系统的初始状态和终止状态，根据离散事件驱动机制产生和更新离散故障事件序列，通过故障事件演化树分析系统状态的更新结果，当离散故障事件序列中所有事件分析结束或系统状态到达终止态时，结束当轮的仿真；当仿真的次数到达规定值后，结束整个仿真过程。

在每一轮的仿真中，DEET 方法会获得一个指定时刻的系统状态观测值，在完成数量足够多的仿真轮数后，DEET 方法获得一个大样本的系统状态观测值并可评估出系统在指定时刻处于某个系统状态的概率。设在第 i 轮仿真中，IMA 平台到达工作时刻 t 处于的状态为 S_t，当仿真的总轮数为 N_{sum} 时，系统在 t 时刻处于状态 S_i 的状态概率 P_{Si} 评估方法为

$$P_{Si} = \frac{1}{N_{sum}} \sum_{i=1}^{N_{sum}} k_{Si} \tag{3}$$

式中，$k_{Si} = \begin{cases} 1 & S_t = S_i \\ 0 & \text{其他} \end{cases}$。

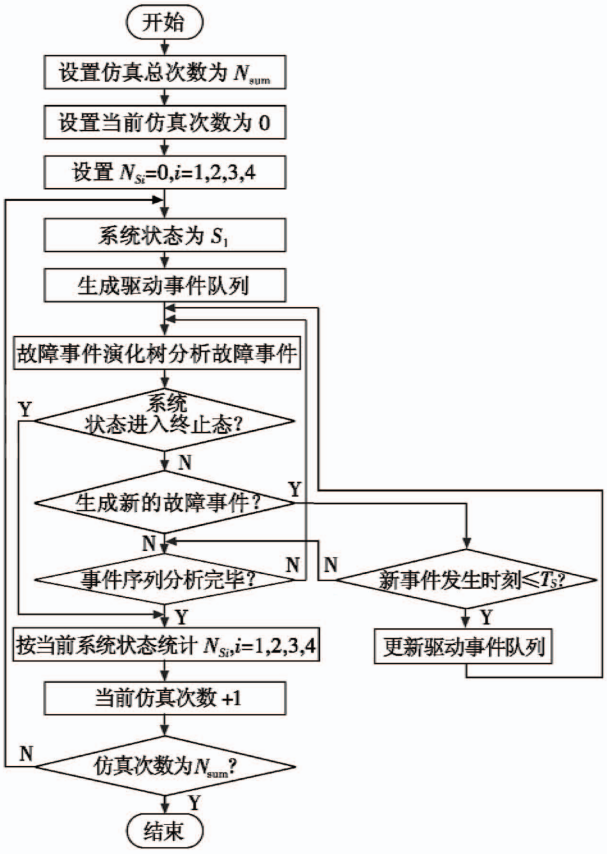

图 4　DEET 方法仿真流程

Fig. 4　Simulation flow of DEET method

3　案例分析

采用 DEET 分析方法对图 1 所示的 IMA 平台在不同时刻处于不同状态的概率进行仿真分析，仿真采用 Python 语言实现，设置工作 GPM 数量为 5，备件 GPM 数量为 2，交换网络为由两块热备份 SW 组成的双余度网络，设置 GPM，SW 和 TM 的故障符合指数分布，GPM，SW 和 TM 的 MTBF 都为 2000 h，即式(2)中的各部件 i 的故障概率密度函数 $f_i(t) = \lambda e^{-\lambda t}$，$\lambda = (5E-4)/h$，在每轮仿真过程中，GPM，SW 和 TM 通过式(2)确定自己的故障事件发生时间，式(2)中的 $g(f_i(t))$ 函数通过 python 语言 numpy 库的随机抽样函数实现。通过本文所述的离散事件驱动机制和故障事件演化树分析 IMA 平台在故障演化过程中时序相关、功能依赖关系和每个故障事件引起的系统状态的变化。记录每轮仿真中在指定时刻 t 系统所处的状态 S_i，在完成了 $N_{sum} = 1 \times 10^5$ 次仿真后，统计在指定时刻 t 系统处于状

态 S_i 的次数，通过式(3)计算系统在 t 时刻的状态概率 P_{Si}，仿真结果如表2所示，可看出采用DEET方法不仅可以分析出系统处于初始状态和完全失效的概率，还可以分析出系统处于需维修但不影响业务以及可完成部分业务状态的概率，相对于传统仅支持正常/故障两态分析的方法，本文方法的分析结果更全面，更有利于IMA平台的业务优化和维修资源的规划。

表2 仿真分析结果

Table 2 Simulation analysis result %

状态概率	工作时间/h				
	200	400	600	800	1000
P_{S1}	49.414	24.897	12.132	6.073	3.077
P_{S2}	46.22	58.432	54.904	44.368	32.93
P_{S3}	3.436	13.423	26.401	38.449	48.453
P_{S4}	0.93	3.248	6.563	11.11	15.54

图5为GPM备件数量为1或2，TM的MTBF为500 h或2000 h，即故障概率密度函数 $f_i(t)=\lambda e^{-\lambda t}$ 中，$\lambda=(2E-3)/h$ 或 $\lambda=(5E-4)/h$，其余仿真条件不变时IMA平台在不同工作时间可完成全部业务的业务可靠度比较结果，即处于 S_1 状态的概率 P_{S1} 与处于 S_2 状态的概率 P_{S2} 之和。从图5可看出，随着备件数量的增加，IMA平台可完成全部业务的业务可靠度提高；此外，TM部件的MTBF提高对整个IMA平台业务可靠性的提高效果十分显著，这是由于重构时GPM的业务迁移需要依赖TM完成，当TM在GPM之前发生故障，IMA平台不能进行重构，导致业务能力降低；因此，作为IMA平台中的可靠性关键部件，应设法提高TM的可靠性或采用冗余TM设计。

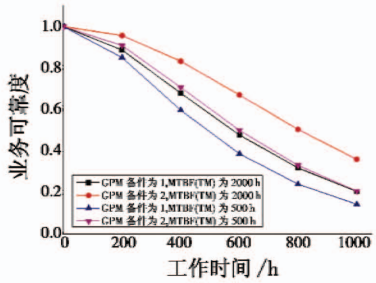

图5 不同条件下的业务可靠度

Fig. 5 Task reliability in different conditions

4 总结

本文的方法通过分析IMA故障演化中时序相关及功能依赖的动态关系，实现IMA平台业务可靠性的准确定量评估，发现IMA平台薄弱环节，为IMA平台的设计改进提供理论数据依据。DEET方法不仅可用于IMA平台的分析，其建模仿真思想也可以扩展到其他具有时序相关、功能依赖、多态性、部件数量多特点的复杂系统可靠性分析，下一步的研究将进一步改进DEET方法并将其应用于具有多种容错机制的复杂容错IMA平台的可靠性分析。

参考文献

[1] EVELEENS R L C. Integrated modular avionics development guidance and certification considerations[R]. Washington: Radio Technical Commission for Aeronautics, 2005.

[2] 王国庆，谷青范，王淼，等. 新一代综合化航空电子系统构架技术研究[J]. 航空学报，2014, 35(6)：1473-1486.

[3] 陈龙，王立松. IMA重构的功能危害分析方法研究[J]. 计算机工程，2016, 42(6)：151-160.

[4] FAULIN J, JUAN A A. Simulation methods reliability and availability of complex systems[M]. London: Springer-Verlag, 2010.

[5] 孙健，张兴军，董小社. 一种可靠性框图的异构系统可用性评价模型[J]. 西安电子科技大学学报：自然科学版，2016, 43(3)：190-196.

[6] 杨建军，黎放，魏军. 基于功能模型的复杂系统FMEA方法[J]. 海军工程大学学报，2009, 21(4)：103-107.

[7] 周斌，黄元亮，黄威. 基于模块化分解的故障树分析方法[J]. 计算机工程，2015, 4(2)：141-144.

[8] LISNIANSKI A, FRENKEL I. Recent advances in system reliability[M]. London: Springer, 2012.

[9] LI X K, HUANG N, ZHENG X Y. Application based dynamic fault tree method for AFDX network[C]//Annual Reliability and Maintainability Symposium, Tucson, AZ, IEEE, 2016. doi: 10.1109/RAMS.2016.7447995.

[10] 廖瑞金，肖中男，巩晶，等. 应用马尔科夫模型评估电力变压器可靠性[J]. 高电压技术，2010, 36(2)：322-328.

[11] SHAMSI P. Applications of non-Markovian hybrid Petri-nets in power engineering[C]//IECON 2014, USA, IEEE, 2014. doi: 10.1109/IECON.2014.7048481.

[12] SHARDA B, BURY S J. A discrete event simulation model for reliability modeling of a chemical plant[C]// Winter Simulation Conference, USA, IEEE, 2008. doi: 10.1109/WSC.2008.4736260.

[13] JUAN A A, MONTEFORTE A, FERRER A, et al. Applications of discrete-event simulation to reliability and availability assessment in civil engineering structures[C]// Winter Simulation Conference, IEEE, 2009. doi: 10.1109/WSC.2009.5429250.

[14] POOYA P, IVY J, MAZUR L, et al. Assessing the reliability of the radiation therapy care delivery process using discrete event simulation[C]//Winter Simulation Conference, USA, IEEE, 2014. doi: 10.1109/WSC.2014.7019980.

[15] LEE J, TOLMAN M, BORRELLI R A. High reliability safeguards approach to remotely handled nuclear processing facilities: use of discrete event simulation for material throughput in fuel fabrication[J]. Nuclear Engineering and Design, 2017, 324(1)：54-66.