

基于概率模型检测的机电系统动态可靠性评价

侯 翌¹ 杨培林¹ 徐 凯¹ 刘 青² 樊娟妮²

1.西安交通大学机械工程学院,西安,710049

2.西北工业集团有限公司计量理化一中心,西安,710043

摘要:为克服传统动态可靠性分析方法的不足,提出基于概率模型检测的机电系统动态可靠性评价方法。介绍了概率模型检测的概念及概率模型检测工具 PRISM。用形式化建模语言描述系统单元的状态变迁过程,建立了机电系统的形式化模型。利用连续随机逻辑对机电系统可靠性评价指标进行形式化描述,建立了可靠性指标的规约表达式,借助概率模型检测工具自动解算可靠性指标,实现了基于概率模型检测的机电系统动态可靠性评价。所提方法建模过程简单,能有效提高机电系统动态可靠性分析的效率。

关键词:动态可靠性;可靠性评价;概率模型检测;机电系统

中图分类号:TH122

DOI:10.3969/j.issn.1004-132X.2019.05.007

开放科学(资源服务)标识码(OSID):



Dynamic Reliability Evaluation Approach for Electromechanical Systems
Based on Probabilistic Model Checking

HOU Yi¹ YANG Peilin¹ XU Kai¹ LIU Qing² FAN Juanni²

1.School of Mechanical Engineering,Xi'an Jiaotong University,Xi'an,710049

2.No.1 Center of Measuring and Physical-chemical Performance Testing,Northwestern
Industrial Group Co.,Xi'an,710043

Abstract: To overcome the shortcomings of the traditional dynamic reliability analysis methods, a dynamic reliability evaluation approach for electromechanical systems was proposed based on probabilistic model checking. The concept of probabilistic model checking and a probabilistic model checker PRISM were introduced. State transitions of system components were represented using formal modeling language provided by the model checker, from which the formal model of electromechanical systems was built. Reliability indices were described by means of continuous stochastic logic formulas to establish the formal specifications of the reliability indices. Based on the formal model and formal specifications, reliability indices were computed automatically with the probabilistic model checker, and therefore dynamic reliability evaluation was achieved based on probabilistic model checking. The approach presented herein simplifies the modeling processes and improves the efficiency of dynamic reliability analysis for electromechanical systems.

Key words: dynamic reliability; reliability evaluation; probabilistic model checking; electromechanical system

0 引言

随着机电一体化技术的发展,机电系统的集成度和复杂程度越来越高,不仅机电系统的性能会随时间发生变化,而且系统组成单元之间往往具有复杂的耦合关系,因此机电系统的动态可靠性越来越引起人们的关注。

目前对系统动态可靠性进行分析评价的主要方法有状态空间法、动态故障树分析(dynamic fault tree analysis,DFTA)法、Petri 网等^[1-2]。状

态空间法以马尔可夫(Markov)模型为基础,通过求解状态转移方程计算系统可靠性指标,但当系统规模较大时,直接应用马尔可夫过程理论建立系统的可靠性模型比较困难^[3]。DFTA 在传统故障树分析(fault tree analysis,FTA)的基础上增加了一些用于描述动态特性的逻辑门,如功能相关门、顺序强制门、优先与门等,在一定程度上加强了其动态描述性能,并通过转化为马尔可夫模型或动态贝叶斯网络得到了定量结果^[4-6],但当系统较复杂时,动态故障树建模困难。Petri 方法具有图形化建模和定量数学计算的优点,可以利

用马尔可夫过程理论或蒙特卡罗 (Monte Carlo) 仿真计算可靠性指标,但系统较复杂时,也会增加 Petri 网的建模难度^[7]。

模型检测是一种形式化的自动验证技术,用于检验有限状态系统是否满足某种给定性质^[8-11]。概率模型检测是对模型检测的拓展,它不仅能够验证系统性质的正确性,还能够自动计算系统性质出现的概率^[12-13]。本文对概率模型检测进行了介绍并将其引入机电系统的动态可靠性评价中,通过对机电系统可靠性问题的形式化建模、可靠性指标的形式化规约,利用概率模型检测工具自动计算可靠性指标,实现基于概率模型检测的机电系统动态可靠性评价。

1 模型检测及概率模型检测

模型检测是一种形式化方法,它首先以某种形式化语言对系统状态变迁进行描述,即对系统进行形式化建模,然后以时序逻辑公式描述所期望的某种性质,即建立性质的形式化规约,最后利用模型检测工具来搜索系统模型的有穷状态空间,自动检验系统是否满足所期望的性质。当系统不满足所期望的性质时,将给出反例说明性质为何不成立。

概率模型检测中的形式化模型是一种随机模型,它反映了系统状态变迁的随机特性。概率模型检测也需要利用包含概率信息的时序逻辑语言对所要验证的性质进行描述,如“系统处于某状态的概率小于 0.001”等,因此通过概率模型检测不仅可以判断某性质是否会发生,而且能计算该性质发生的概率。

概率模型检测可以通过概率模型检测工具 PRISM 来进行^[14]。作为一种广泛使用的概率模型检测工具,PRISM 支持多种概率模型,如连续时间马尔可夫链 (continuous time Markov chains, CTMC)、马尔可夫决策 (Markov decision processes, MDP)、概率时间自动机 (probabilistic timed automata, PTA) 等。PRISM 采用二叉决策图 (binary decision diagram, BDD) 和多端二叉决策图 (multi-terminal binary decision diagram, MTBDD) 两种数据结构,并融合了图论计算和数值计算两类计算技术,所以可以构建和计算非常大的系统可达状态空间,并有很高的数值计算效率,适用于复杂系统的概率模型检验。

2 可靠性指标形式化规约及可靠性评价

为了基于概率模型检测实现机电系统的动态

可靠性评估,本文利用 PRISM 提供的形式化建模语言建立机电系统的形式化模型,用连续随机逻辑 (continuous stochastic logics, CSL) 对机电系统的可靠性指标进行形式化规约。

2.1 机电系统的形式化建模

概率模型检测工具 PRISM 提供的形式化建模语言包括模块 (modules) 和变量 (variables) 两种基本元素^[14]。模型由一个或多个模块构成,一个模块包含一个或多个变量,变量用来描述状态。模块的定义形式为

module name
:
endmodule

模块的行为通过命令 (commands) 来定义,命令由守卫 (guard) 和更新 (update) 组成,命令的形式为

[] guard \rightarrow prob: update

一条命令反映了一次状态变迁过程,其中 guard 描述的是状态变迁需要满足的条件,当条件满足时便可进行状态的变迁 (更新)。update 为变迁 (更新) 后的状态,状态变迁过程的状态转移率由 prob 表达。命令前面的方括号 [] 中可添加执行标记,标记相同的命令是同步执行的。

对机电系统进行形式化建模时,每个组成单元用一个模块来描述,各个模块组成整个系统的形式化模型。模块中的命令反映了单元状态的变迁条件、变迁后的状态及状态转移率等信息。对于动态可靠性中的相关失效问题,单元失效之间的关联性可在变迁条件中进行描述。

2.2 可靠性指标的形式化规约及可靠性评价

PRISM 支持多种形式化规约语言,对基于 CTMC 的系统形式化模型,PRISM 用连续随机逻辑 CSL 来描述所期望的性质。由于系统的状态变迁过程都对应一条状态路径,因此 CSL 定义了状态公式和路径公式,分别用于描述系统所处的状态及状态在路径上的时序关系。

状态公式的巴科斯范式为

$$\neg \varphi :: true \mid a \mid \varphi \wedge \varphi \mid \neg \varphi \mid S_{\sim c}[\varphi] \mid P_{\sim c}[\psi] \quad (1)$$

其中, a 表示每个原子公式都是状态公式; 符号 \wedge 和 \neg 分别表示逻辑与和逻辑非; “ \sim ”表示运算符, $\sim \in \{<, >, \leq, \geq\}$, $S_{\sim c}[\varphi]$ 表示状态 φ 成立的概率满足比较运算符指定的约束 c , $P_{\sim c}[\psi]$ 表示路径 ψ 成立的概率满足比较运算符指定的约束 c 。

路径公式的巴科斯范式为

$$\neg \psi :: X^i \varphi \mid \varphi_1 U^i \varphi_2 \quad (2)$$

其中,“X”和“U”为时态算子,分别表示“下一步”和“直到”, $X^I\varphi$ 描述了从当前状态下经过时间段 I 进入状态 φ ; $\varphi_1U^I\varphi_2$ 表示在时间段 I 内,状态 φ_1 一直成立直到状态 φ_2 成立。

PRISM 对 CSL 进行了扩展,在路径公式中添加了时态算子“G”(表示全局)和“F”(表示将来某时刻),同时引入操作符“ $P=?$ ”和“ $S=?$ ”分别用于描述一个路径公式成立的概率以及一个状态的稳态概率。另外 PRISM 对逻辑运算符作了重新定义,如用“&”表示“ \wedge ”,用“ \leq ”表示“ \leq ”等。

对机电系统进行可靠性评价时,对所关注的系统状态用上述状态公式进行规约,并用路径公式规约相应的可靠性指标。例如若关注某系统“单元 R 处于状态 r 并且单元 Q 处于状态 q ”这一状态在时间 t 内出现的概率,则针对这一评价指标建立的 CSL 规约表达式为

$$P=?[F=t \ R=r \& \ Q=q] \tag{3}$$

式(3)表示时间 t 内“单元 R 处于状态 r 并且单元 Q 处于状态 q ”的概率是多少。

将上述机电系统的形式化模型及可靠性指标的 CSL 规约表达式输入概率模型检测工具 PRISM,即可针对 CSL 规约表达式进行模型检验并能自动求解表达式成立的概率,从而实现可靠性评价。

3 实例分析

图 1 为某五轴联动数控机床主轴箱的驱动系统示意图。系统通过安装平衡油缸来平衡主轴箱的自重,从而减轻电机、丝杠和轴承等部件的负载。当平衡油缸正常工作时,由于平衡油缸的平衡作用,滚珠丝杠及轴承所受负载较小。当平衡油缸系统由于某种原因造成油液泄漏而使油缸支撑失效时,丝杠和轴承 2(推力轴承)会承受比油缸正常工作时更大的负载(轴承 1 为向心轴承,忽

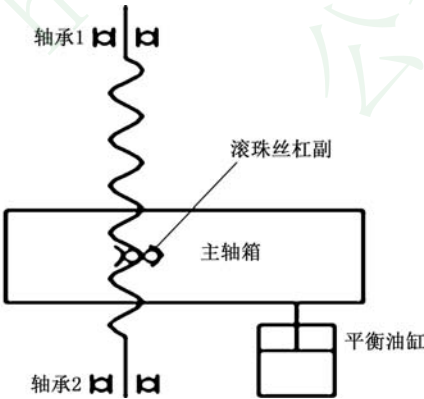


图 1 主轴箱驱动系统原理

Fig.1 Principle of spindle box drive system

略油缸对其影响),其寿命也会随之下降,即由于平衡油缸的失效会加剧其他部件的失效,因此该系统的失效为相关失效。

设所有部件的寿命服从指数分布,平衡油缸的失效率为 $8(10^{-6} \text{ h}^{-1})$,其他部件的失效率如表 1 所示。

表 1 各部件的失效率

Tab.1 The failure rate of each part 10^{-6} h^{-1}

	平衡油缸正常	平衡油缸故障
滚珠丝杠	9	20
轴承 1	16	16
轴承 2	16	45

上述主轴箱驱动系统的正常工作条件是滚珠丝杠、轴承 1 及轴承 2 正常工作,平衡油缸的作用只是减缓系统的失效。按照前文提到的方法,可以建立系统的形式化模型,如图 2 所示。其中平衡油缸对轴承 2 和滚珠丝杠失效的影响体现在相应的状态变迁条件中,见图 2b 和图 2d 所示的模型。

```
module balance_cylinder
bc:[0..1] init 0; // 0: 正常; 1: 失效
[]bc=0 -> 8e-6:(bc'=1); //平衡油缸状态变迁
endmodule
```

(a)平衡油缸模型

```
module ballscrew
ba:[0..1] init 0;
[] ba=0 & bc=0 -> 9e-6:(ba'=1);
//平衡油缸正常时滚珠丝杠状态变迁
[] ba=0 & bc=1 -> 20e-6:(ba'=1);
//平衡油缸故障后滚珠丝杠状态变迁
endmodule
```

(b)滚珠丝杠模型

```
module bear1
b1:[0..1] init 0;
[] b1=0 -> 16e-6:(b1'=1);
endmodule
```

(c)轴承 1 模型

```
module bear2
b2:[0..1] init 0;
[] b2=0 & bc=0 -> 16e-6:(b2'=1);
//平衡油缸正常时轴承状态变迁
[]b2=0 & bc=1 -> 45e-6:(b2'=1);
//平衡油缸故障后轴承状态变迁
endmodule
```

(d)轴承 2 模型

图 2 主轴箱驱动系统形式化模型

Fig.2 Formal model of spindle box drive system

依据主轴箱驱动系统的正常工作条件,可建立如下的可靠性评价指标形式化规约:

$P=? [F=t \text{ } ba=0\&b1=0\&b2=0]$ (4)

式(4)表示主轴箱驱动系统在时间 t 内正常工作的概率,即可靠度。依据上述形式化模型及可靠性指标形式化规约,通过 PRISM 进行模型检测,可求得系统可靠度,如图 3 所示。

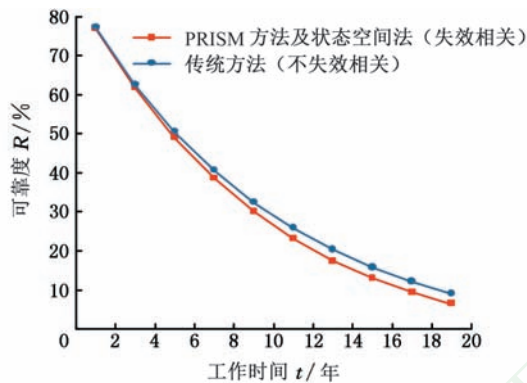


图 3 主轴箱驱动系统可靠度

Fig.3 Reliability of spindle box drive system

为了验证上述计算结果的正确性,本文也用状态空间法^[15]对此进行计算。该实例涉及四个组成单元(平衡油缸、滚珠丝杠、轴承 1 及轴承 2),考虑每个单元有正常与失效两种状态,四个单元组成的系统共有 $2^4 = 16$ 个状态。根据状态之间的转移率(失效率)可画出状态转移图并据此建立 16×16 阶的状态转移密度矩阵 A (限于篇幅,状态转移图及转移密度矩阵在此不再列出),由状态空间法建立如下的矩阵微分方程:

$\frac{d}{dt}P(t)=P(t)A$ (5)

$P(t)=(p_1(t), p_2(t), \cdots, p_{16}(t))$

其中, $P(t)$ 为系统状态行向量。

求解该微分方程组,可得系统处于正常状态的概率(可靠度)为

$R=\frac{5}{4}e^{-49 \times 10^{-6}t}-\frac{1}{4}e^{-81 \times 10^{-6}t}$ (6)

式(6)的计算结果与基于 PRISM 的计算结果完全一致,如图 3 所示。

在该实例中,若不考虑失效相关性,即不计平衡油缸失效对其他部件失效的影响,则可按传统方法计算系统的可靠度。由于滚珠丝杠、轴承 1 及轴承 2 在功能上是串联关系,可得到不考虑失效相关时的系统可靠度为

$R(t)=R_{bs} \cdot R_{b1} \cdot R_{b2}=e^{-9 \times 10^{-6}t} \cdot e^{-16 \times 10^{-6}t} \cdot e^{-16 \times 10^{-6}t}=e^{-41 \times 10^{-6}t}$ (7)

式中, R_{bs} 、 R_{b1} 、 R_{b2} 分别为滚珠丝杠、轴承 1 和轴承 2 的可靠度。

主轴箱驱动系统可靠度计算结果如图 3 所示。可以看出在不考虑失效相关时计算得到的系统可靠度要大于考虑失效相关时所得到的可靠

度,这会使可靠性评价产生较大的偏差。

4 结论

(1)利用模型检测工具提供的形式化建模语言可以描述系统单元的状态变迁过程,单元失效之间的关联性可体现在状态变迁条件中。

(2)只需分别建立各个单元的状态变迁模型(模块),即可构建出整个系统的形式化模型,系统建模过程简单方便。

(3)通过对可靠性指标的形式化规约,借助模型检测可自动计算各种可靠性指标,提高了可靠性评价的效率。

参考文献:

[1] DISTEFANO S, PULIAFITO A. Reliability and Availability Analysis of Dependent-dynamic Systems with DRBDs[J]. Reliability Engineering & System Safety, 2009, 94(9): 1381-1393.

[2] 陶俊勇,王勇,陈循. 复杂大系统动态可靠性与动态概率风险评估技术发展现状[J].兵工学报,2009,30(11):1533-1539.

TAO Junyong, WANG Yong, CHEN Xun. A Survey of the Complex Large System Dynamic Reliability and Dynamic Probabilistic Risk Assessment[J]. Acta Armanentarii. 2009,30(11):1533-1539.

[3] 张振友,郭强,黄立坡,等. 基于马尔可夫过程的武器系统相关失效分析[J]. 火力与指挥控制, 2012, 37(7): 117-119.

ZHANG Zhenyou, GUO Qiang, HUANG Lipo, et al. Analysis of Weapon Systems Subject to Correlative Cause Failures Based on Markov Process[J]. Fire Control & Command Control, 2012, 37(7): 117-119.

[4] BOUISSOU M, BON J L. A New Formalism that Combines Advantages of Fault-trees and Markov Models: Boolean Logic Driven Markov Processes [J]. Reliability Engineering & System Safety, 2003: 82(2): 149-163.

[5] CHIACCHIO F, COMPAGNO L, D'URSO D, et al. An Open-source Application to Model and Solve Dynamic Fault Tree of Real Industrial Systems [C]//IEEE International Conference on Software. Benevento, Italy, 2012: 1-8.

[6] MONTANI S, PORTINALE L, BOBBIO A, et al. A Tool for Automatically Translating Dynamic Fault Trees into Dynamic Bayesian Networks[C]// IEEE Reliability & Maintainability Symposium. Newport Beach, USA, 2006: 434-441.

[7] 石健,王少萍,王康. 基于 GSPN 的机载液压作动

- 系统可靠性模型[J]. 航空学报, 2011, 32(5): 920-933.
- SHI Jian, WANG Shaoping, WANG Kang. GSPN-based Reliability Model of Aircraft Hydraulic Actuator System[J]. Acta Aeronautica et Astronautica Sinica, 2011, 32(5): 920-933.
- [8] CLARKE E M, GRUMBERG O, PELED D A. Model Checking [M]. Cambridge: MIT Press, 2000.
- [9] 林惠民, 张文辉. 模型检测: 理论、方法与应用[J]. 电子学报, 2002, 30(12A): 1907-1912.
- LIN Huimin, ZHANG Wenhui. Model Checking: Theories, Techniques and Applications[J]. Acta Electronica Sinica, 2002, 30(12A): 1907-1912.
- [10] 贾仰理, 李舟军, 邢建英, 等. 基于模型检验的构件验证技术研究进展[J]. 计算机研究与发展, 2011, 48(6): 913-922.
- JIA Yangli, LI Zhoujun, XING Jianying, et al. Advances in the Component Verification Technology Based on Model Checking[J]. Journal of Computer Research and Development, 2011, 48(6): 913-922.
- [11] KWIATKOWSKA M, NORMAN G, PARKER D. Controller Dependability Analysis by Probabilistic Model Checking[J]. Symposium on Information Control Problems in Manufacturing, 2004, 15: 112-119.
- [12] KWIATKOWSKA M. Model Checking for Probability and Time: from Theory to Practice[C]//Logic in Computer Science, Proceedings of 18th Annual IEEE Symposium. Ottawa, Canada, 2003: 351-360.
- [13] GRUNSKA L, COLVIN R, WINTER K. Probabilistic Model-checking Support for FMEA[C]//Quantitative Evaluation of Systems, Fourth International Conference on the Quantitative Evaluation of Systems. Edinburgh, UK, 2007: 119-128.
- [14] KWIATKOWSKA M, NORMAN G, PARKER D. PRISM 4.0: Verification of Probabilistic Real-time Systems[C]//Proc. 23rd International Conference on Computer Aided Verification. Snowbird, USA, 2011: 585-591.
- [15] 杨蔚百, 熊景寰, 孙启宏. 电力系统可靠性分析基础及应用[M]. 北京: 水利电力出版社, 1986: 147-149.
- YANG Shibai, XIONG Jinghuan, SUN Qihong. Foundation and Application of Power System Reliability Analysis [M]. Beijing: China Water Power Press, 1986: 147-149.
- (编辑 王艳丽)
- 作者简介: 侯 翌, 男, 1992 年生, 硕士研究生. 研究方向为机电系统可靠性及结构强度. E-mail: hy920314@126.com. 杨培林 (通信作者), 男, 1963 年生, 教授. 研究方向为机电系统可靠性与动力学、机器人等. E-mail: plyang@mail. xjtu.edu.cn.
- ~~~~~
- (上接第 548 页)
- PANG Hui, LIANG Jun, WANG Jianping, et al. Adaptive Fuzzy Sliding Mode Control for Vehicle Active Suspension Systems Considering System Uncertainty [J]. Vibration and Impact, 1988, 37(15): 261-269.
- [13] 刘金琨, 孙富春. 滑模变结构控制理论及其算法研究与进展[J]. 控制理论与应用, 2007(3): 407-418.
- LIU Jinkun, SUN Fuchun. Research and Development on Theory and Algorithms of Sliding Mode Control[J]. Control Theory and Application, 2007(3): 407-418.
- [14] 高远, 范健文, 谭光兴, 等. 汽车悬架系统混沌运动的自适应反演滑模控制[J]. 中国机械工程, 2013, 24(11): 1531-1537.
- GAO Yuan, FAN Jianwen, TAN Guangxing, et al. Control for Chaos in Automobile Suspension System Based on Back-stepping Design Adaptive Sliding Mode Controller[J]. China Mechanical Engineering, 2013, 24(11): 1531-1537.
- [15] 李政, 胡广大, 崔家瑞, 等. 永磁同步电机调速系统的积分型滑模变结构控制[J]. 中国电机工程学报, 2014, 34(3): 431-437.
- LI Zheng, HU Guangda, CUI Jiarui, et al. Sliding-mode Variable Structure Control with Integral Action for Permanent Magnet Synchronous Motor [J]. Chinese Journal of Electrical Engineering, 2014, 34(3): 431-437.
- [16] 寇发荣, 王哲, 杜嘉峰, 等. 电动静液压作动器主动悬架力跟踪控制研究[J]. 中国机械工程, 2017, 28(24): 2964-2970.
- KOU Farong, WANG Zhe, DU Jiafeng, et al. Study on Force Tracking of EHA Active Suspension[J]. China Mechanical Engineering, 2017, 28(24): 2964-2970.
- (编辑 袁兴玲)
- 作者简介: 寇发荣, 男, 1973 年生, 教授、博士. 研究方向为车辆振动与主动控制. 发表论文 60 余篇. E-mail: koufarong@xust.edu.cn.