应用 Stateflow 技术的安全性建模与仿真

王 蓓 赵廷弟

(北京航空航天大学 可靠性与系统工程学院, 北京 100191)

摘 要: 为了保障高风险系统的使用安全性,探索事故的运动规律与应急决策,提出了面向事故过程的安全性仿真方法,并结合有限状态机原理与 Stateflow 技术设计了建模方法与仿真机制,该方法能实现混合系统过程状态逻辑与连续机理的建模与仿真,仿真结果能反映事故发展过程中系统的状态-时间特性、人机交互特性以及过程机理,为应急决策提供定量的依据. 最后,对某产品实例的事故过程进行了模型设计与仿真实验,验证了该仿真方法的有效性与合理性.

关 键 词: 系统安全性; 仿真; 模型设计; 混合系统

中图分类号: N 945

文献标识码: A **文 章 编 号**: 1001-5965(2011)11-1415-06

Safety simulation applying Stateflow technology

Wang Bei Zhao Tingdi

(School of Reliability and Systems Engineering, Beijing University of Aeronautics and Astronautics, Beijing 100191, China)

Abstract: The accident-process oriented safety simulation method was proposed to ensure the safety of high risk systems, as well as explore the movement during the accident evolution and emergency treatment. The modeling and simulation method was designed upon the principle of finite state machine and the technology of Stateflow. By this method, the modeling and simulation of process logic and continues mechanism in hybrid system can be achieved. Then the simulation result can reflect the system characteristic of state transforming and man-machine communicating, and the mechanism in the accident process, accordingly, the quantitative support can be provided for the emergency treatment decision-making. Finally, the model design and simulation experiment for the typical accident process in some product were implemented, and the validity and rationality of this proposed method were validated by the result .

Key words: system safety; simulation; model building; hybrid systems

开展系统安全性研究旨在识别、控制和消除风险,提高产品的安全性水平. 日益发展的仿真技术为系统安全性研究提供了新的途径. 常用的安全性仿真方法大多基于概率分布的纯逻辑仿真,存在一定的局限性:基于故障树、事件树模型的安全性仿真应用蒙特卡罗原理[1-4],能实现系统的故障分析与安全性风险评估,但在解决包含时间、过程变量、人的操作行为等动态因素的问题上还存在一定不足;基于 Petri 网和 Markov 模型[5-7]的安全性仿真考虑系统的状态变化的离散性和动态性,但难以反映复杂系统的连续变化机理.

文献[8]认为,系统中存在反映物理过程的连续时间特性和反映事件驱动过程变化的离散特性,而系统又是一个包含任务目标、软硬件设备、人的行为、环境和管理因素等 5 类成分以及相互关系的整体[9],系统事故发展与应急过程的研究则更具综合性.

系统的复杂性使得系统的使用过程具有离散-连续混合特征,离散和连续两种运动模式交互作用[10-11],因此,提出基于有限状态机理论的安

收稿日期: 2010-07-20; **网络出版时间**: 2011-11-23 15:06; **DOI**: CNKI:11-2625/V.20111123.1506.011
网络出版地址: www.cnki.net/kcms/detail/11.2625.V.20111123.1506.011.html
基金项目: 国防预研资助项目(51319040201)
作者简介: 王 蓓(1985 -),女,湖北武汉人,硕士生,wangbei3414@126.com.

全性仿真方法,面向具有连续-离散特性的混合系统进行建模,并在 Simulink/Stateflow[12-14] 平台中实现,通过仿真模拟系统的事故发展动态规律与状态-时间特性,为应急预案的设计与人员应急训练提供定量的依据,弥补传统仿真方法的不足.

1 面向事故过程的安全性仿真

事故是系统运动的一种表现形式,事故在系统运动中发生,取决于系统的动态特性. 因此,完整认识事故发生的规律,需要研究系统发生事故的运动特征. 面向事故过程的安全性仿真是从系统事故过程着眼,对事故发展与应急操作过程进行动态的模拟与分析,探索事故发展过程中系统的运动特性,为确定准确的应急措施提供依据,为操作人员的训练提供平台.

对于一些复杂的高风险系统,直接进行事故过程的实物演练是危险的而不允许的. 用仿真的方法来研究事故过程模型,能有效地实现对这类系统的事故分析与应急训练. 这类研究过程的仿真称之为"过程仿真",它是在一定的初始条件和输入条件下,动态执行过程模型,考察系统的输出以及各种性能指标,它是一种动态的执行过程,用于模拟过程的抽象行为.

为了将系统信息反映在计算机中,需建立合理的数学模型,面向事故分析的模型是能反映复杂系统行为的逻辑和连续时间模型. 系统模型可抽象为两类层次,低一层的模型为系统的物理模型,需要用连续方程进行描述,高一层的模型为离散的行为逻辑模型,可以用有限状态机、模糊逻辑、PETRI 网等进行描述,此外,还包括两类层次模型的耦合关系. 面向事故过程仿真的主要步骤见图 1.

图 1 给出了面向事故过程的仿真的基本流程,可见模型的构建与相互耦合关系是仿真过程中的重点. 选择有限状态机的图形实现工具 Stateflow 构建离散的逻辑模型. 同时,Simulink 强大的函数处理和仿真能力适合于处理子系统物理方程,二者融合不失为面向事故过程的安全性仿真的有效途径.

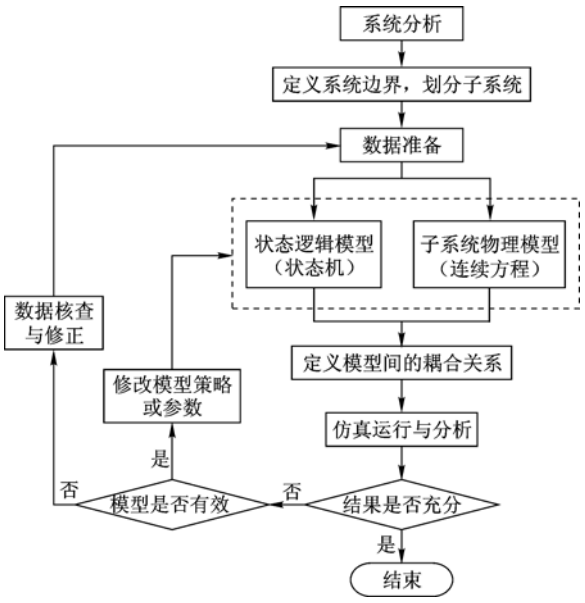


图 1 面向事故过程的仿真步骤

2 基于 Stateflow 的安全性仿真

2.1 Stateflow 原理[15]

Stateflow 是有限状态机的图形实现工具,它使用流程图和状态转移图等概念,用以解决复杂的监控逻辑问题. Stateflow 是嵌入到 Simulink 中的,能够对 Simulink 建模的实际系统中目标的状态变化进行动态控制,实现二者的无缝连接. Stateflow 图表由图形对象和非图形对象构成,图形对象包括状态(state)、转移(transition)、节点(junction)等,非图形对象包括事件(event)、数据(data)、目标对象(target). 图 2 是 Stateflow 图表的基本结构.

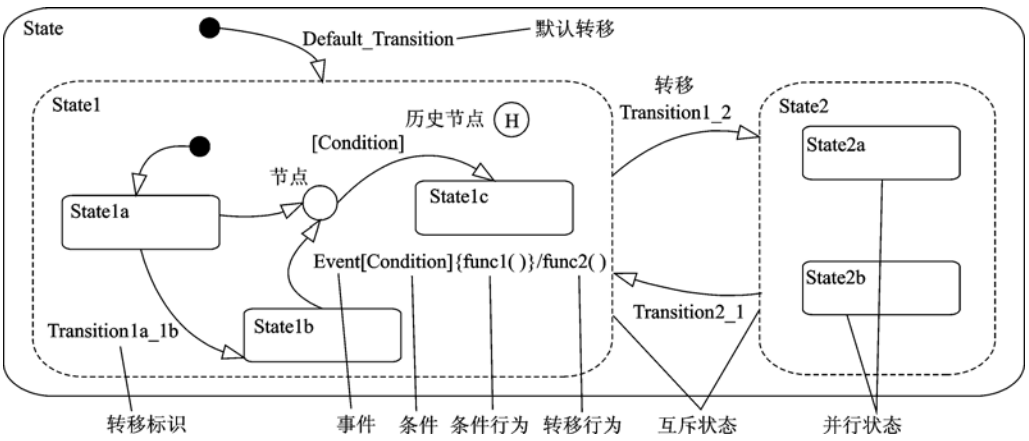


图 2 Stateflow 图表的基本结构

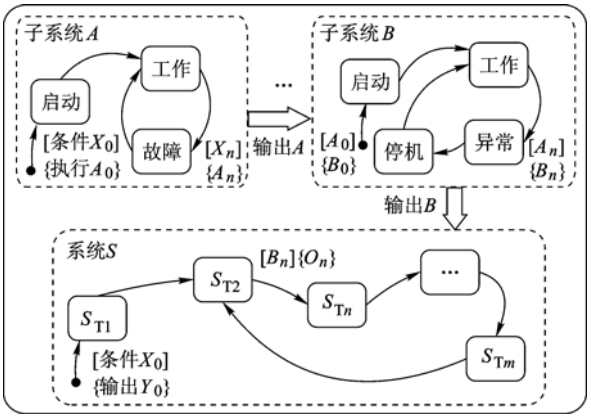
在 Stateflow 图表中,状态用圆角矩形表示,能体现层次关系、并行关系以及历史记录的功能. 状态是系统的运行模态,有“激活”与“非激活”两种模式. 转移定义系统的逻辑信号流向,用来联系任意两个图形目标、状态或节点. 利用转移和节点就可以很方便地设计开发出复杂的逻辑.

事件和数据不在图表中呈现,需要在 Stateflow Explorer 中定义和修改. 事件可以触发转移的发生和行为的执行,数据用来存储图表中涉及到的数字变量. 输入输出事件和数据与 Simulink 之间可以实现相互的通讯连接.

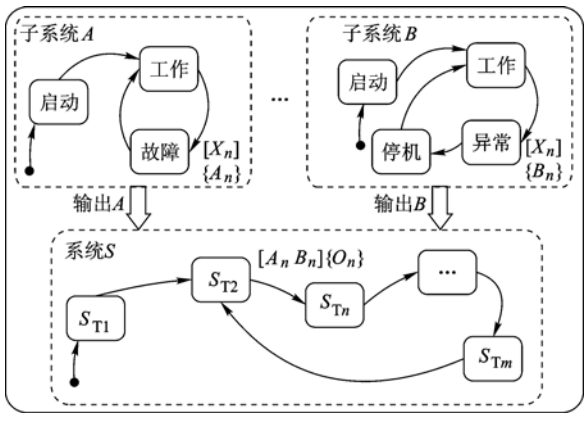
2.2　基于 Stateflow 的事故逻辑模型

构建面向危险事故过程的离散逻辑模型,需要 Stateflow 模型中的组成元素进行定义,其基本元素定义如下:①状态(S_T);②输入(X);③输出(Y);④状态转移函数(f);⑤输出函数(g).

图 3 给出了用 Stateflow 建模语言描述一个包含若干子系统的系统 S 运行过程中的状态变化模型的示意图.



a　串行影响模式



b　并行影响模式

图 3　Stateflow 事故逻辑模型

图 3a 和图 3b 分别是串行和并行耦合系统的状态机模型. 每个子系统包含多个状态、转移弧、输入和输出信息,并作为独立的状态机进行封装,通过输入输出信息与其他子系统形成交互. S_T 为整机系统 S 运行过程中的状态,当该系统模型开始运行时,所有子系统的状态都处于他们的正常模式,当子系统的状态发生变化时,向系统 S 输入相应的执行函数,满足相应的判定条件则发生状态转移.

Stateflow 的输入信息来源于 Simulink 模型,包括反映系统变量-时间连续变化的物理模型与人员的应急操作模型. 通过输入数据建立相应的条件,触发系统状态转移. Stateflow 的输出信息为系统使用过程中需监测的物理量或相应的函数,传输到 Simulink 中,在输出模块中显示.

2.3　仿真平台体系结构

在 Simulink/Stateflow 环境下进行安全性仿真的体系结构如图 4 所示,通过 Simulink 与 Stateflow 之间的无缝连接实现系统中连续物理模型与离散状态逻辑模型的耦合仿真.

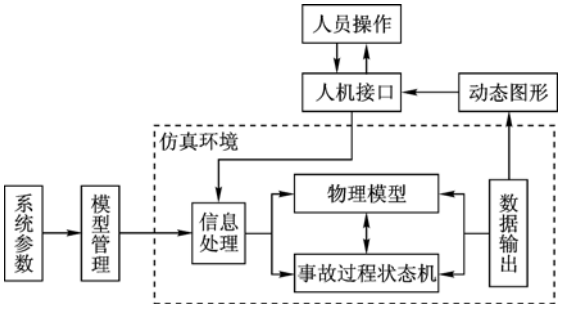


图 4　安全性仿真体系结构

首先处理系统使用过程的相关数据信息,在 Simulink 中构建反映系统变量-时间连续变化的物理模型,为 Stateflow 的运行提供输入信息,构成状态转移的条件. 通过时钟脉冲触发 Stateflow 模块的时序运行. 操作人员依据 Stateflow 模块的实时输出来进行判断与决策,从而通过人机交互模块形成反馈,为 Stateflow 提供新的输入,驱动新的状态转移的执行.

通过这种方式实现离散-连续混合过程的动态控制,一方面运用 Stateflow 实现系统状态的动态控制,构建系统正常工作和失效与应急处理过程中的状态变化模型;另一方面,与 Simulink 环境下的模型形成数据接口,进行离散、连续模型的动态仿真,从而实现系统事故过程的模拟与分析.

3　应用实例

以某产品发电机舱的事故过程为例,应用 Stateflow 进行事故过程仿真,通过仿真再现事故过程的动态时间特性与人机交互特性,实现该建模仿真方法的应用.

3.1 系统分析与模型设计

在某产品发电机舱室环境中,发电机及附属设备是主要的危险源,机体和电路设备常因疏于维修等原因导致老化或故障,当舱室中润滑油类物质遇高温又极易引发火灾,因此舱室火灾是主要事故隐患,若不及时控制,可能造成整个产品瘫痪. 对该产品进行层次划分,子系统层为发电机子模块、电路控制子模块,系统层为舱室系统子模块. 针对因电路故障引起的火灾事故过程,建立系统 Stateflow 模型如图 5 所示. 图 5 中,用 3 个相对独立的 Stateflow 图分别建立发电机子系统、电路控制子系统、舱室系统的有限状态机模型,其中,舱室系统属于顶层系统,它们有各自的控制逻辑,同时又通过数据与事件的传输、条件判断与转移行为的执行实现子系统与系统之间的耦合关系.

当仿真开始执行时,所有的系统都进入初始状态,并完成系统初始化,随后依次判断转移条件是否满足而执行相应的状态转移,如模型所示,舱室系统的启动依赖于发电机子系统和电路控制子系统的状态量(dystate 和 ecstate),若当前时钟达到电控系统的失效时间([current_time >= time*A*]条件满足),则电路控制子系统进入失效状态,此时,发电机子系统随之进入过热状态. 依次类推,图 5 所示的模型建立了发电机舱室中系统间的耦合关系和事故过程的动态行为.

在 Simulink 中构建仿真平台如图 6 所示,将 Stateflow 生成的控制逻辑嵌入到 Simulink 模型中,实现事件流、数据流和时间流的传输与驱动. 图 6 中,以并行的开关模块作为操作员模型,可以在仿真执行过程中执行相应的操作,包括启动电磁阀的开启、关闭、发电机的加载、应急灭火操作,构成系统的"事件流";电路控制子系统失效模型、发电机温度模型和燃烧放热模型分别为 Stateflow 输入相应的"数据流";采用周期为 2 s 的均匀脉冲作为时钟触发,即仿真运行的时间步,构成系统的"时间流".

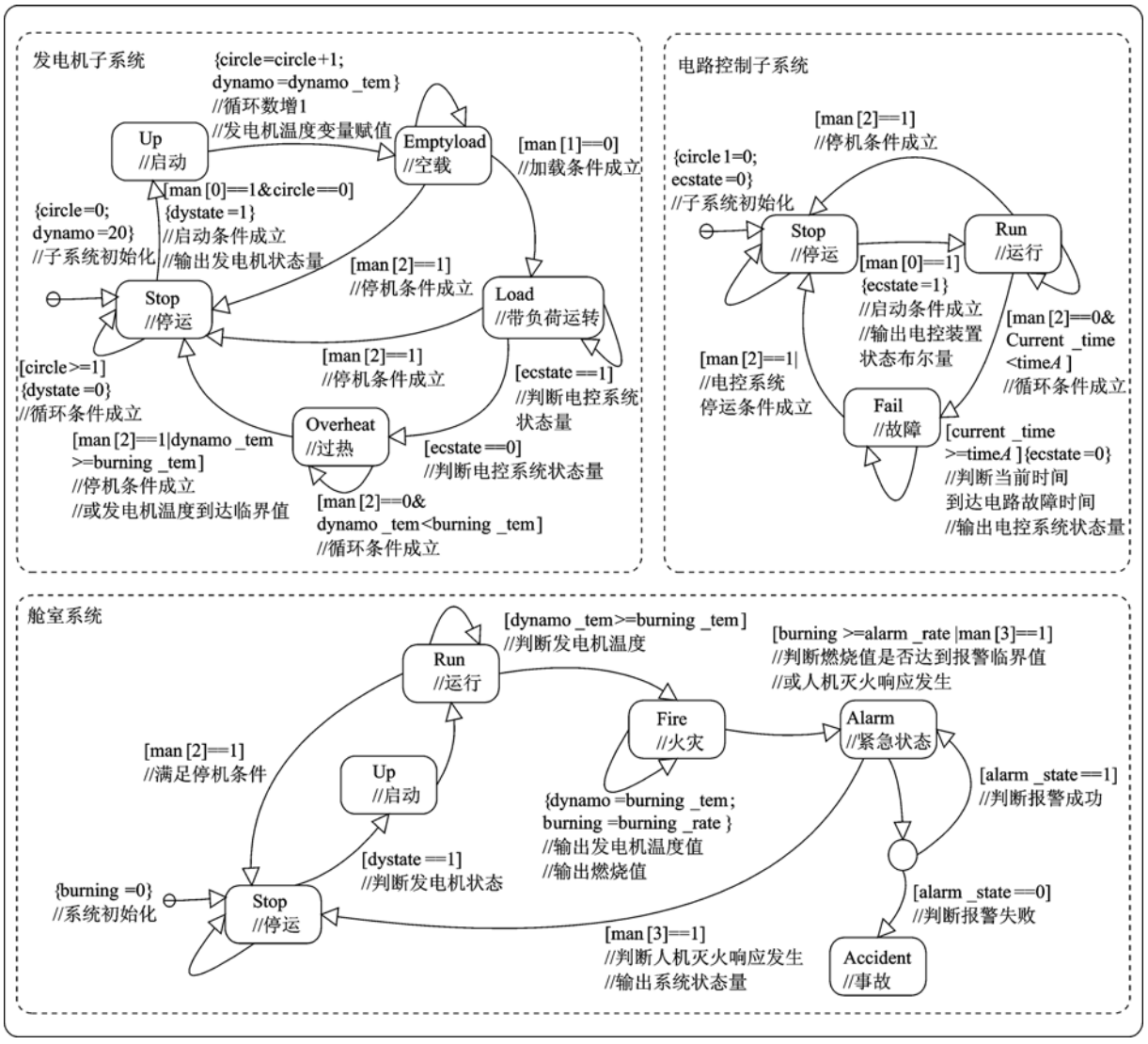


图 5 某发电机舱事故过程 Stateflow 模型

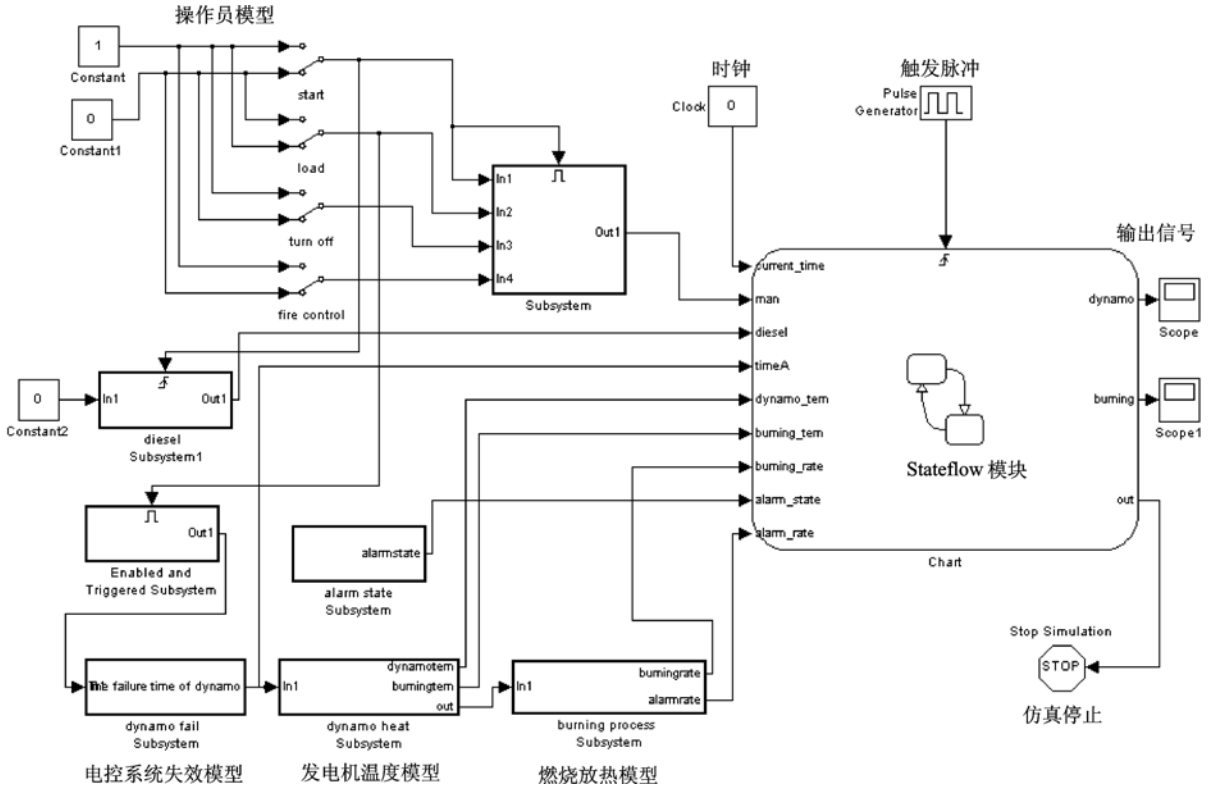


图 6　仿真系统的 Simulink 模型

3.2　仿真运行与结果分析

在此平台下运行仿真,分别模拟事故过程和有应急处置操作的过程中系统的状态变化过程,选取两次仿真中系统的状态曲线分别如图 7 所示,事故过程曲线模拟事故发展过程中系统的输出状态,该过程中,人员启动柴油发电机系统并加载发电机,随后,发电机因故障而导致温度升高,随即发生火灾,过程中人员并未采取任何应急措施,最后造成系统事故. 应急处置过程曲线模拟了事故发生发展过程中人员采取应急操作时,系统的状态输出.

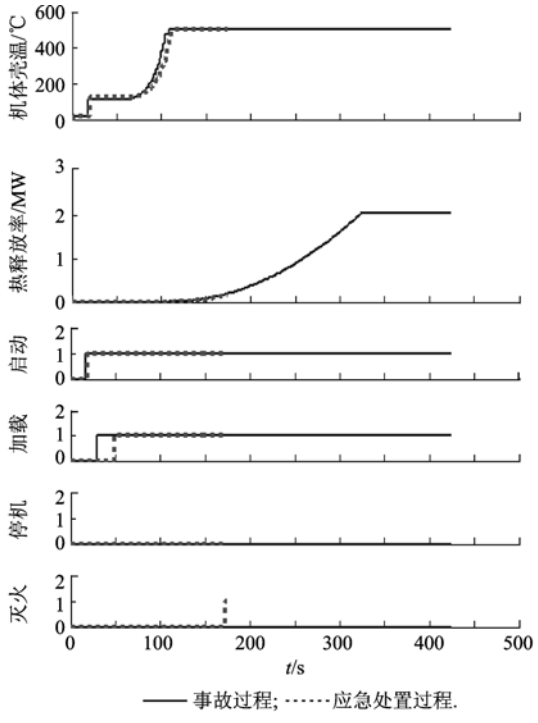


图 7　系统的状态-时间变化曲线

仿真结果反映了事故状态变化规律,即该发电机舱由出现故障到发生火灾事故的整个过程中的状态变化趋势,也反映发展过程中用户通过采取应急操作对系统状态变化的监控与抑制作用,从而保证系统向安全状态转移.

4　结　论

1）提出了面向事故过程的安全性仿真技术,为解决复杂高风险系统的事故模拟与分析问题提供了新的途径,为安全性仿真领域做出了新的探索.

2）将 Simulink/Stateflow 仿真平台成功运用于安全性仿真,提出了安全性仿真中的建模思路和设计方法,体现了应用 Simulink/Stateflow 构建安全性仿真平台的适用性.

3）将该仿真方法应用于某产品的事故过程实例,通过仿真为事故发展过程的动态规律提供了定量的模拟与分析,验证了该建模仿真方法的合理性与科学性.

参考文献（References）

[1] 孙殿阁,孙佳,王淼,等. 基于 Bow-tie 技术的民用机场安全风险分析应用研究[J]. 中国安全生产科学技术,2010,6(4):85 - 89
Sun Diange, Sun Jia, Wang Miao, et al. Application of the improved Bow-tie risk analysis technology in civil airport safety [J]. Journal of Safety Science and Technology, 2010, 6(4): 85 - 89(in Chinese)

[2] 曾声奎,赵廷弟,张建国,等. 系统可靠性设计分析教程[M]. 北京:北京航空航天大学出版社,2001:117 - 157
Zeng Shengkui, Zhao Tingdi, Zhang Jianguo, et al. System reliability design and analysis tutorial[M]. Beijing: Beijing University of Aeronautics and Astronautics Press, 2001: 117 - 157 (in Chinese)

[3] 李堂经,王新阁,许卓然. 基于蒙特卡洛仿真的动态故障树分析[J]. 兵工自动化,2010,29(3):42 - 46
Li Tangjing, Wang Xinge, Xu Zhuoran. Dynamic fault tree analysis based on Monte Carlo simulation[J]. Ordnance Industry Automation, 2010, 29(3): 42 - 46(in Chinese)

[4] 马振宇. 电网可靠性的蒙特卡洛仿真研究[J]. 电力系统保护与控制,2009,37(14):55 - 67
Ma Zhenyu. Research of Monte Carlo simulation for power system reliability assessment[J]. Power System Protection and Control, 2009, 37(14): 55 - 67(in Chinese)

[5] Hachtel G D, Macii E, Pardo A, et al. Markovian analysis of large finite state machines[J]. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 1996, 15(12): 1479 - 1493

[6] 孟海宁,齐勇,侯迪. 基于非马尔可夫随机 Petri 网的软件再生建模与分析[J]. 计算机学报,2007,30(12):2212 - 2217
Meng Haining, Qi Yong, Hou Di. Modeling and analysis of software rejuvenation Based on non-Markovian stochastic Petri nets [J]. Chinese Journal of Computers, 2007, 30(12): 2212 - 2217 (in Chinese)

[7] 韩用明,吴相林,岳超源. 基于 SPN 的软件过程模型及蒙特卡洛仿真[J]. 华中科技大学学报,2003,31(7):37 - 39
Han Yongming, Wu Xianglin, Yue Chaoyuan. Model of software process and Monte-Carlo simulation analysis based on SPN[J]. Journal of Huazhong university of Science and Technology, 2003, 31(7): 37 - 39(in Chinese)

[8] Polic A, Hace A, Jezernik K. A recursive description of mixed time-and event-driven dynamic in mechatronic Systems[J]. 5th IEEE International Conference on Industrial Informatics, 2007, 19(11): 293 - 298

[9] Williams J H. NAS system engineering manual[M]. Version 3.1. Washington: FAA System Engineering Council, 2006: 4 - 6

[10] Rooney B D. Hybrid launch system vehicles, ground facilities and operations integration[R]. AIAA 2006-7231, 2006

[11] 张悦,王东风,韩璞,等. 一类混杂系统的推广自动机模型及其仿真[J]. 系统仿真学报,2007,19(15):3546 - 3549
Zhang Yue, Wang Dongfeng, Han Pu, et al. Extended automata model and simulation for a class of hybrid systems[J]. Journal of System Simulation, 2007, 19(15): 3546 - 3549(in Chinese)

[12] 黄永安,马路,刘慧敏. MATLAB 7.0/Simulink 6.0 建模仿真开发与高级工程应用[M]. 北京:清华大学出版社,2005
Huang Yongan, Ma Lu, Liu Huimin. MATLAB 7.0/Simulink 6.0 modeling simulation and advanced engineering application [M]. Beijing: Tsinghua University Press, 2005(in Chinese)

[13] 陈桂明,张明照,戚红雨,等. 应用 MATLAB 建模与仿真[M]. 北京:科学出版社,2001
Chen Guiming, Zhang Mingzhao, Qi Hongyu, et al. Apply MATLAB to modeling and simulation[M]. Beijing: Science Press, 2001(in Chinese)

[14] Barnard P A. Graphical techniques for aircraft dynamic model development[R]. AIAA 2004-4808, 2004

[15] The MathWorks Inc. Stateflow and Stateflow coder for use with Simulink[M]. USA: The MathWorks Inc Copyright, 2006

（编　辑:赵海容）