航 空 学 报
Acta Aeronautica et Astronautica Sinica
Nov. 25 2011 Vol. 32 No. 11 2016-2024
ISSN 1000-6893 CN 11-1929/V
http://hkxb.buaa.edu.cn hkxb@buaa.edu.cn
文章编号:1000-6893(2011)11-2016-09

基于混合动态系统理论的事故过程建模方法

王薇,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:为了研究系统事故机理,建立有效的事故过程模型,分析了事故过程的特征,指出其呈现离散与连续动态行为交互的混合特性。针对现有事故过程建模方法在描述该混合特性时的不足,提出了基于混合动态系统理论的建模方法,建立了事故过程的混合自动机模型,在 Simulink/Stateflow 环境下进行仿真。实现了事故过程的连续机理与状态运转及其交互影响的有效融合,为制定应急预案提供了依据。通过案例模拟了系统从危险经应急操作,直至事故或安全的过程,验证了该方法的有效性。

关键词:事故;安全工程;建模;混合动态系统;自动机理论;Simulink

中图分类号:V328;N945 **文献标识码**:A

建立事故过程模型是研究事故发生、发展机理的重要手段,是制定应急预案、事故预防的基础。对于由相互联系的人员、装备、环境等构成的系统而言,系统因动态平衡受到扰动而处于危险状态,当未采取有效控制使系统状态超出了安全约束范围时则发生了事故[1-2]。事故过程建模的实质是研究系统从危险演化到事故的动态行为机制。

目前以事件树分析(ETA)、事件序列图(ESD)、Petri 网模型、有限状态机模型等[3-6]建立的事故过程模型能够表征系统人员行为、装备、环境因素随时间的变化,以分析由于逻辑或时序上的演变导致的事故,反应了系统事故过程中的离散动态特征。而随着研究的深入,事故与系统性能的联系日趋紧密,事故过程的动态行为不仅具有离散特征,还包含了体现系统性能的物理过程变量在控制措施下的动态运转。概率动力学理论能够综合系统的离散状态与物理过程两部分,不同状态下服从不同的物理过程规律,通过计算与物理过程变量相关的状态转移概率,驱动系统在不同状态间运行,评估出现不期望状态的概率,并在核电安全评估等领域有广泛应用[7-8]。以此为基础的动态事件树分析(DETA)和动态逻辑分析方法(DYLAM)以仿真求得状态转移概率的数值解[9-10],该类方法中的物理过程变量用于计算状态转移概率而不是作为独立的建模对象,在建立事故过程中系统物理过程变量对人员行为、环境因素等作用的响应时存在一定不足。针对直观描述事故过程中系统状态与物理过程变量及其相互作用的动态行为机制,混合动态系统理论提供了一种有效的建模思路[11-16]。

因此,本文提出了基于混合动态系统理论的事故过程建模方法,通过以混合自动机建立的事故过程模型表现系统的混合特性,并在 Simulink/Stateflow 平台上进行仿真,验证方法的有效性。

收稿日期:2011-03-08;**退修日期**:2011-04-25;**录用日期**:2011-07-18;**网络出版时间**:2011-08-10 11:18
网络出版地址:www.cnki.net/kcms/detail/11.1929.V.20110810.1118.003.html **DOI**:CNKI:11-1929/V.20110810.1118.003
* **通讯作者**.Tel.:010-82316570 E-mail:ztd@buaa.edu.cn

引用格式:王薇,赵廷弟. 基于混合动态系统理论的事故过程建模方法[J].航空学报,2011,32(11):2016-2024. Wang Wei, Zhao Tingdi. Research on accident process modeling based on hybrid dynamic system theory [J]. Acta Aeronautica et Astronautica Sinica, 2011, 32(11): 2016-2024.

1 事故过程特性分析

1.1 事故过程的离散动态特性

事故过程的研究对象是危险发生后,采取人员应急操作或装备自动保护等一系列具有时序性、规则性的调节措施,系统状态被控制在安全范围内或超出安全范围发生事故的这一过程,是系统状态运转的过程。人员应急操作是指定时刻通过人机交互作用对系统作出调整;装备自动保护是指定时刻装备自动作出调整行为。这两种行为均在离散的时间点上发生,因此这两类行为可视为具备离散特征的序列。

包含交互协调的人员、装备、环境等因素的系统中,"状态"体现了系统所处的条件或状况,是对系统特征的描述;"事件"是引发状态变化的瞬间动作,是人员操作或装备的自动保护等系统调节措施。系统事故过程起源于危险状态,其后系统的调节措施作为离散事件,使系统的状态也在离散的时刻上发生变化。在此基础上发生下一离散事件,系统状态继续变化[17]。这种具有离散动态特性的事故过程可表达为[18]

$$\mathrm{DEDS}=\{\Xi_{\mathrm{in}},\Xi_{\mathrm{out}},S_{\mathrm{a}},\Sigma,\Delta,\Omega\}$$

式中:Ξ_{in}为输入集合;Ξ_{out}为输出集合;S_{a}为事故过程中的离散状态集合;Σ为事故过程中的离散事件集合;Δ为发生Σ后系统的状态转移规则,$\Delta:S_{\mathrm{a}}\times\Sigma\rightarrow S_{\mathrm{a}}$;$\Omega$为系统输出函数,$\Omega:S_{\mathrm{a}}\times\Xi_{\mathrm{in}}\rightarrow\Xi_{\mathrm{out}}$。系统从初始状态开始运行,当满足一定条件时事件发生,则系统此时状态由当前事件和前一状态决定,并在下一事件发生前维持不变。

因此,事故过程是由事件驱动的系统状态的运转过程,具有离散动态特性。

1.2 事故过程的连续动态特性

事故过程是系统状态的运转,体现了系统状态在系统调节措施下从危险状态运转到安全或事故状态的动态特征[8]。系统安全或事故采用系统状态变量来度量,当系统状态变量位于安全界限内时系统安全,超出安全界限则发生事故[19]。因此事故过程中的系统状态变量呈现动态特征。

假设系统在某状态时有k个描述安全的状态变量$h_1(t),h_2(t),\cdots,h_k(t)$,则该状态在$[t_0,t_l]$内的任意时间点$t_i=t_0+i\cdot\Delta t(i=1,2,\cdots,l)$处的一系列状态变量为

$$\boldsymbol{H}=\begin{bmatrix}h_1(t_0) & h_2(t_0) & \cdots & h_k(t_0)\\ h_1(t_1) & h_2(t_1) & \cdots & h_k(t_1)\\ \vdots & \vdots & & \vdots\\ h_1(t_l) & h_2(t_l) & \cdots & h_k(t_l)\end{bmatrix}\tag{1}$$

式中:t_0为初始时刻;Δt为时间间隔;$h_j(t_i)$($j=1,2,\cdots,k$;$i=1,2,\cdots,l$)为变量h_j在t_i时刻的值[20]。

由人员、装备、环境交互作用而构成的系统属于广义的物理系统,表征系统安全与否的系统状态变量是具有物理含义的系统性能参数。系统的工作过程以及应对危险的调节过程均属于物理过程,性能参数遵循所属的各种状态的物理规律,其变化行为可用微分方程形式描述,即式(1)中的每个变量$h_j(j=1,2,\cdots,k)$为连续状态变量,在$[t_0,t_l]$内满足

$$\dot{h}_j=f_{\mathrm{a}}(h_j,u_{\mathrm{a}})$$

式中:u_{a}为外部输入变量。

因此事故过程中,系统的性能参数作为系统状态变量,具有连续动态特性。

1.3 事故过程的混合动态特性

由前述分析可知,事故过程可以抽象为一个系统状态的离散变化过程,但系统状态与涉及系统性能的连续状态变量联系紧密。而完全把事故过程处理成连续变量的动态过程,又忽略了系统在事故过程的不同阶段遵循的连续规律的差异。因此单独采用离散事件动态系统或连续变量动态系统都不能完整地描述事故过程的特性,事故过程兼具离散和连续两类动态特征。

同时,在事故过程中,系统的离散与连续动态特性又具有新的交互特性。一方面,人员操作、装备故障、环境变化等事件都发生在特定的时间点上,导致系统的状态呈离散跳变,系统状态变化使系统连续状态变量服从的连续规律也发生变化。以由人员、电炉和房间组成的系统为例,系统的状态变量为房间温度,温度过高或过低均为危险状态。温度过高后的某时刻,人员采取应急操作将电炉断电,系统由加热状态变为散热状态,房间温度变化服从的规律也会发生变化。另一方面,当表现系统特征的系统连续状态变量满足一定条件

时,也会驱使系统状态发生改变。仍以本节中的系统为例,当房间温度过低,保护装置工作,电炉自动接通,系统由散热状态进入加热状态。因此事故过程中包含的离散和连续动态过程是相互影响的,事故过程呈现离散、连续特征交互作用的混合动态特性。

因此事故过程模型需要实现以下 3 个功能:①描述系统状态的离散变化;②描述状态变量的连续变化;③离散状态与连续状态变量相互影响,从而推动模型运转。

2 混合动态系统理论及其在事故过程建模中的应用

2.1 混合动态系统模型的组成

混合动态系统模型包含离散系统、连续系统和接口 3 类对象。在建立离散和连续动态模型基础上,通过接口在二者之间建立映射关系,从而实现离散和连续系统数据间的交互[11-13]。

图 1 为适用于事故过程的混合动态系统模型的组成图,定义了模型中各组分的内容以及数据间的联系。

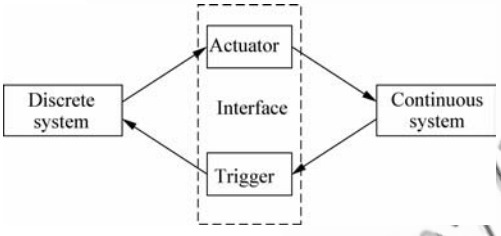


图 1 混合动态系统基本组成结构

Fig. 1 Basic frame of hybrid dynamic system

图 1 中的连续系统部分以微分方程描述。$\boldsymbol{x}_c \in \mathbf{R}^n$、$\boldsymbol{r}_c \in \mathbf{R}^m$ 和 $\boldsymbol{z}_c \in \mathbf{R}^p$ 分别为系统中的连续状态变量、输入变量和输出变量,并且满足:$\dot{\boldsymbol{x}}_c = f_c(\boldsymbol{x}_c, \boldsymbol{r}_c)$,$f_c: \mathbf{R}^n \times \mathbf{R}^m \to \mathbf{R}^n$;$\boldsymbol{z}_c = g_c(\boldsymbol{x}_c)$,$g_c: \mathbf{R}^n \to \mathbf{R}^p$ 为连续变量的输出函数。

离散系统部分以三元组$\{Q, \Pi, \delta\}$描述,其中 Q 为系统状态集合;Π 为事件集合;δ 为状态转移函数,$\delta: Q \times \Pi \to Q$。

接口部分包括执行器和触发器。执行器定义了广义映射 $\gamma: X \to \Pi$,表示从连续变量集合到离散事件集合的映射。触发器定义了广义映射 $\alpha: Q \to X$,表示从离散状态集合到连续系统间的映射。

2.2 事故过程的建模

2.2.1 事故过程的混合自动机模型

在混合动态系统基本结构基础上,采用混合自动机实现事故过程模型的运转。该模型表示为一个八元组:

$$\mathrm{HA} = \{X, U, Y; S; E, f, \mathrm{Inv}; \mathrm{Init}\}$$

式中:X、U 和 Y 分别为混合自动机中的连续状态变量集合、输入变量集合和输出变量集合;S 为混合自动机中的离散状态集合;E 为事件;f 为混合自动机中的连续状态变量服从的连续规律;Inv 为混合自动机中的离散状态到连续变量间的映射;Init 为混合自动机中的初始状态集合。

混合自动机内的组元表征了事故过程的离散、连续和交互特征。

在建立混合自动机模型前,首先要对系统及系统任务进行深入的分析,包括:系统功能,系统中人员、装备、环境的交互关系与结构层次;系统任务运行原理;任务过程描述及阶段划分;任务过程涉及的影响安全的因素、各因素间的关系等。例如研究飞行过程中的安全问题,应明确驾驶员、飞机及其相关系统、环境间的关系以及运行原理。明确飞行过程中,可能导致飞行事故的因素分类,如天气原因、设备故障等。

随后,需要确定事故过程建模的起点,即系统发生的危险。根据危险对于系统性能最直接的影响,确定本次建模所针对的系统特征。例如选取由于大气扰动造成的飞行事故为研究对象,则大气扰动作为危险是建模的起点,其对飞行最为关键的影响是造成飞行运动特征的突变,有导致事故的可能。

然后,对应于本次建模所需研究的系统特征,通过任务分析,确定表征系统是否发生事故的系统状态变量,使其作为事故过程模型的输出变量。例如大气扰动后的飞行安全研究,选取飞行运动学参数作为系统状态变量。

接下来,应明确本次建模仿真中,对于是否发生事故的判据,即处于安全状态界限内的系统状

态变量取值范围,在大气扰动飞行的例子中,可以规定某时刻下飞行速度、高度、过载的安全范围。

在明确以上建模前提与假设的基础上,可以根据事故过程的实际信息,构造混合自动机模型 HA 的八元组,具体内容如下:

(1) 构造表征离散特征的组元 S

根据前期工作的系统分析,确定危险发生后的应急措施流程,以实施的先后顺序,确定系统随之产生的各个状态,状态表征了系统对于应急操作或环境扰动的响应。在此基础上,考虑应急操作成功或失败,增加系统状态,构成整个事故过程中,系统可能出现的全部离散状态。八元组中以 S 为离散状态集合,状态 S 的具体内容与人员、装备、环境等因素有关。例如大气扰动下的飞行安全研究中,可能出现的系统状态有顺风飞行、手动油门飞行、自动油门飞行、撞地事故等。

(2) 构造表征连续特征的组元 X、U 和 Y

在前期工作中,已经明确了最终用于判别是否发生事故的状态变量总集,此时应落实每一离散状态时,系统中运行的连续变量以及输出变量。八元组中以 X 为连续状态变量集合,$X=\{x_1, x_2, \cdots, x_m\}$ 是系统运行中的实际物理参量,即连续系统模型所计算的状态变量,例如飞行高度、俯仰角等。八元组中以 Y 为输出变量集合,$y \in Y$ 是用来监测和进行结果分析的连续变量,用于在每一状态时判别是否发生事故,例如飞行速度、高度和过载等。

在此基础上,应确定每一状态的连续状态变量运行所需设定的输入变量,八元组中以 U 为输入变量集合。例如飞行过程中的舵面偏转角度、风速等。

(3) 构造表征交互特征的组元 E、f 和 Inv

在已构造好的离散状态基础上,须为状态间添加转换关系,从而使系统状态运转起来。八元组中以 E 为事件集合,表示系统状态的转移及其发生规则。$e \in E$ 用五元组定义,$e=\langle s, a, \mathrm{Guard}_{ss'}, s' \rangle$。$s$ 和 s' 分别为事件发生前后系统的状态;a 为该事件的编号;$\mathrm{Guard}_{ss'}$ 为事件发生的条件。事件发生的条件用于状态转移的逻辑判断,当满足条件时事件发生,体现了人员应急操作或环境扰动等特征信息,这些信息包含时间值、人员操作的成功或失败、连续状态变量等,以应急操作等提供的信息为依据,以逻辑运算或关系运算的形式表达。例如在某时刻发生的成功切换自动与手动油门操作,系统状态由自动油门飞行转至手动油门飞行,则该事件发生条件为 t 到达指定时刻,且动作信号值表示动作成功,这两者判断均为真时,事件发生;又如在飞行至 100 m 高度时遇到风切变,则该事件发生条件为状态变量高度 $z=100$ m,当该判断为真时事件发生。

接下来确定在事故过程中表示系统处于每一状态时连续状态变量所服从的连续规律,在八元组中以 $\dot{x}=f(x,u)$ 表示,例如手动油门飞行状态下,状态变量为飞行速度、高度等,则连续规律为飞行运动动力学方程组。

Inv 表示离散状态 S 到连续变量 X 间的映射。当 $s \in S$ 时,有 $\mathrm{Inv}(s) \subset X$。

(4) 构造其他组元

Init 为初始状态集合,$\mathrm{Init} \subseteq S \times X$,定义了系统连续状态变量和离散状态的初始值。在事故过程中表示模型起始参数的设置。

2.2.2 模型运转机制

混合自动机模型能够采用有向图的形式描述。图 2 是事故过程的混合自动机模型示意图,图中方框为状态,定义了每个状态下的系统连续变量及其变化规律。箭头线为事件,定义了事件的起始状态和目标状态,以及事件发生条件。虚线圈划分出了各状态在事故过程中的进程。

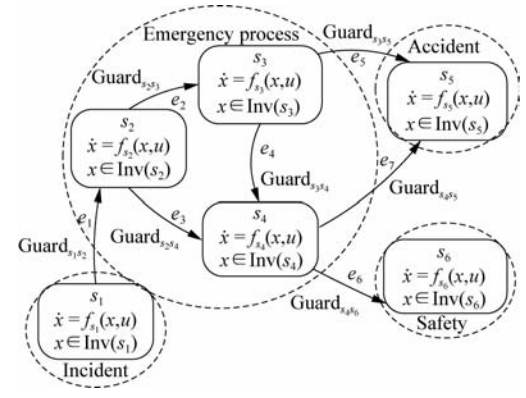


图 2 事故过程的混合自动机模型示意图

Fig. 2 Hybrid automata model of accident process

初始状态 s_1 时系统处于危险中,随着时间的推进,连续状态变量按规则 $\dot{x}=f_{s_1}(x,u)$ 变化。

某时刻人员采取应急操作，在事故过程模型中体现为当状态变量满足条件 $\text{Guard}_{s_1 s_2}$ 时，事件 e_1 发生，此时系统状态变化到 s_2，连续状态变量按规则 $\dot{x}=f_{s_2}(x,u)$ 继续变化。系统对危险状态的控制措施体现为当系统变量满足一定的条件时发生的事件，事件的触发使系统状态跃变，系统连续变量服从的规律也随之发生变化，系统依据此规则持续运转。系统的动态过程中，当系统的状态变量超出规定的安全界限时便发生事故。此模型将事故过程体现为系统动态运转，而运转的机制呈现出系统离散和连续特征交互的动态特性。

2.3 仿真实现

Stateflow 作为 Simulink 平台中提供的图形化建模的仿真工具箱，能够通过状态流程和事件驱动实现事故过程中离散系统部分的建模仿真[21-22]，Stateflow 定义的逻辑能够嵌入到 Simulink 模型中，通过定义输入输出数据实现两者间信息交互，实现混合动态系统的仿真。该环境下建立的事故过程仿真模型运行原理如图 3 所示。

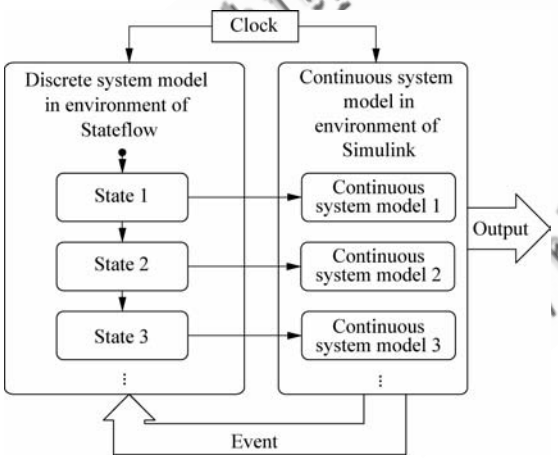


图 3 Simulink/Stateflow 平台下的仿真模型运行原理

Fig. 3 Principle of hybrid system model in environment of Simulink/Stateflow

在 Simulink 中构建连续系统模型，然后根据事故过程的混合自动机模型在 Stateflow 中构建系统的状态变化逻辑。模型运行时，时钟模块分别向这两个模块传递时钟信息，由 Stateflow 的初始状态开始，向 Simulink 输出连续系统模型的选择信号并给该阶段连续变量赋初始值，接着机理模型计算系统连续状态变量，并向 Stateflow 传递变量值，当变量符合事件发生条件时，Stateflow 模块进入下一状态，从而推动仿真模型的运转。

混合动态系统理论能够描述系统状态运转及过程中所涉及的性能机理，从人员、装备、环境交互作用的系统整体角度构建事故过程模型，能够为同类问题建模提供思路。模型所描述的系统状态类型及特征根据危险影响的严重程度选取，建模颗粒度因素决定了模型展现的系统状态特征以及模型复杂程度。

3 应用案例

以简化的飞机下滑穿过逆风区域过程为例，说明该建模方法的使用过程。

3.1 事故过程描述

飞机以一定速度下滑的过程中逆风，在 270 m高度，从逆风区域进入无风区域，飞机的空速减小，高度降低到正常值以下，随后飞行员应断开自动油门并将油门增大，以提高飞行速度。并且断开俯仰角控制系统，并将俯仰角调至 15°，以减小高度骤降[23]。

3.2 建模准备

在系统分析的基础上，提取如下建模信息：

(1) 系统由驾驶员、飞机和大气环境组成。该事故过程所研究的系统特征为飞行运动学参数。

(2) 用于判断安全与否的变量是飞行速度和高度，系统中连续状态变量属于飞行参数，由包含飞行运动动力学模块、控制规律以及风模块的飞行仿真计算得出。

(3) 事故过程中的事件包括人员应急操作和环境变化。按照时间先后顺序，依次为进入无风区、对油门和升降舵两个通道的操作。

(4) 人员操作设定为只有成功与失败两种情况，模型中体现为输入变量 1 与 0。

3.3 混合自动机建模

本例中事故过程的混合自动机模型表示为如下八元组 $\text{HA}=\{X,U,Y;S;E,f,\text{Inv};\text{Init}\}$，构造过程如下：

(1) 状态 $S=\{s_1,s_2,s_3,s_4,s_5,s_6,s_7,s_8\}$,对应于逆风飞行、无风飞行、手控油门飞行、自动油门飞行、手控俯仰角飞行、自动俯仰角飞行、事故、安全。

(2) 以地速、飞行高度、俯仰角以及油门开度作为每一状态下的连续状态变量,即

$$X=\{v,z,\theta,\mathrm{pow}\}$$

(3) 以油门、升降航、副翼、方向舵的输入(d_{th}、d_{e}、d_{a}、d_{r})和风速在 3 个轴系下的分量以及人员操作信号变量(r_manual_throttle、r_manual_pitch)为输入变量。

(4) 以地速和飞行高度作为每一状态下的输出,$Y=\{v,z\}$。

(5) 结合离散状态的分析,以进入无风区、自动油门改成手控油门、自动俯仰角控制改成手动俯仰角控制等应急操作为基准,考虑两次应急操作有成功和失败两种完成效果。本例中各事件列于表 1 中。

(6) 连续状态变量的演化规律 f 由包含飞行运动动力学模块、控制规律以及风模块的飞行仿真模型决定。逆风或无风飞行对应是否接入风模块计算;油门和俯仰角的操作对应控制规律中相应通道的不同控制模式和输入值。

表 1 事件的说明

Table 1 Explanation of events

No.	Previous state	Subsequent state	Guard
1	s_1	s_2	$z<270$ m
2	s_2	s_3	r_manual_throttle=1
3	s_2	s_4	r_manual_throttle=0
4	s_3	s_5	r_manual_pitch=1
5	s_4	s_5	r_manual_pitch=0
6	s_3	s_6	r_manual_pitch=1
7	s_4	s_6	r_manual_pitch=0
8	s_5	s_7	$t=9$ s,55 m/s$<v<$70 m/s
9	s_5	s_8	$t=9$ s,$v<55$ m/s or $v>70$ m/s
10	s_6	s_7	$t=9$ s,55 m/s$<v<$70 m/s
11	s_6	s_8	$t=9$ s,$v<55$ m/s or $v>70$ m/s

3.4 模型运行

图 4 是 Simulink 环境下的事故过程模型。

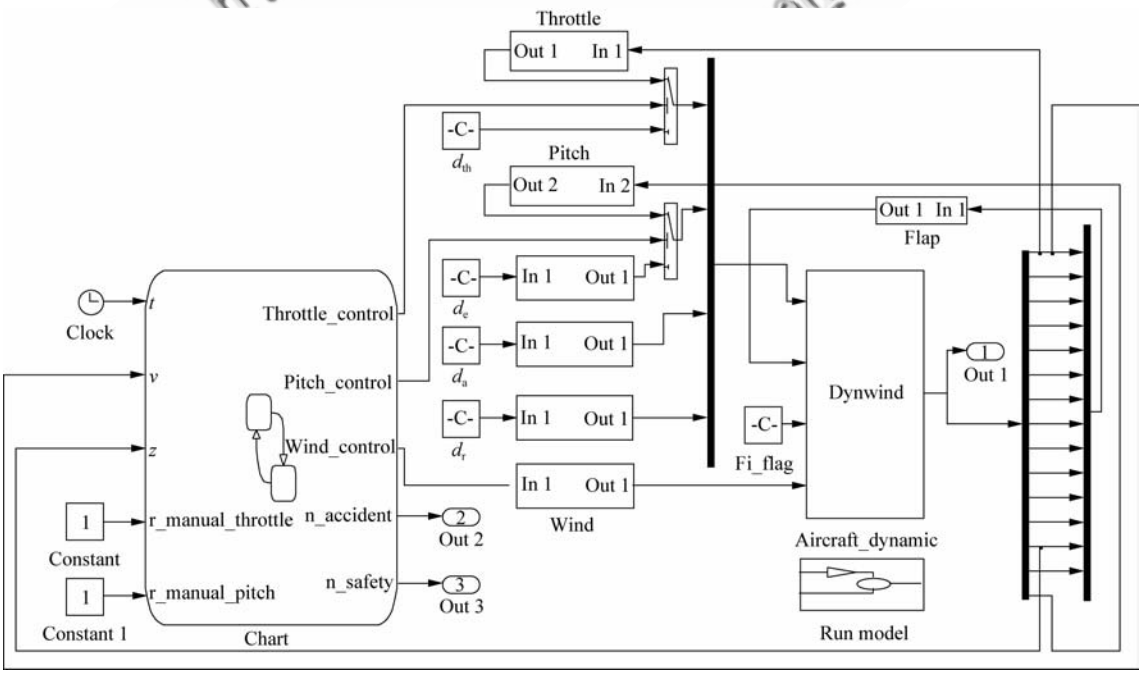


图 4 Simulink 环境下的事故过程模型

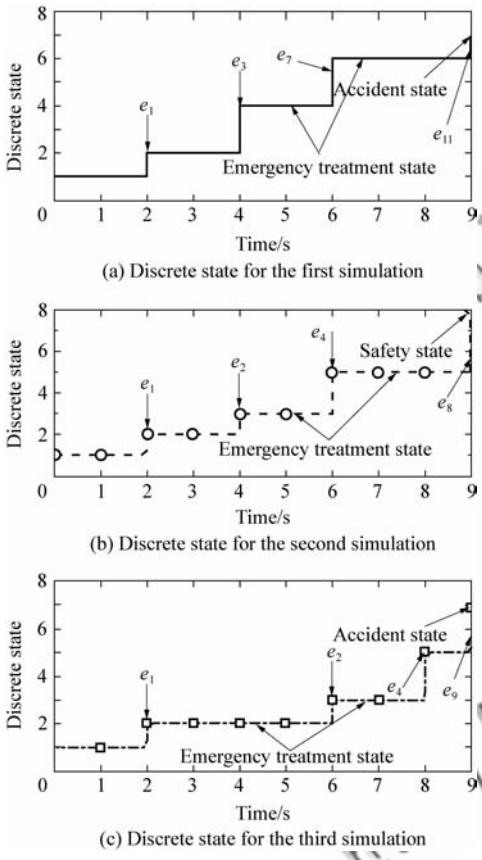
Fig. 4 Accident process model in environment of Simuink

运行此模型,第 1 次仿真,手动油门切换与关闭俯仰角控制系统均失败。第 2 次仿真,第 4 s 手动油门切换,2 s 后关闭俯仰角控制系统。第 3 次仿真,第 6 s 手动油门切换,2 s 后关闭俯仰角

控制系统。

3.5 结果分析

图 5 是 3 次仿真系统离散状态的变化，纵坐标表示离散状态的编号。图 5(a)为第 1 次仿真，两次应急操作均失败，系统状态变化为 $s_1 \rightarrow s_2 \rightarrow s_4 \rightarrow s_6 \rightarrow s_7$。图 5(b)和图 5(c)为第 2 次和第 3 次仿真，两次应急操作均成功，采取操作的时间不同导致应急结果不同。



(a) Discrete state for the first simulation

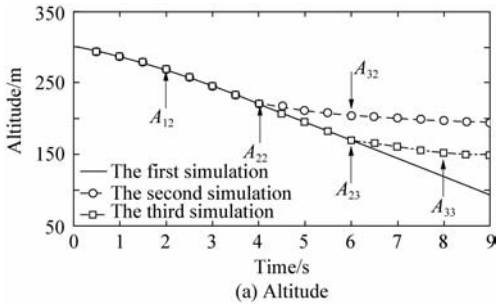
(b) Discrete state for the second simulation

(c) Discrete state for the third simulation

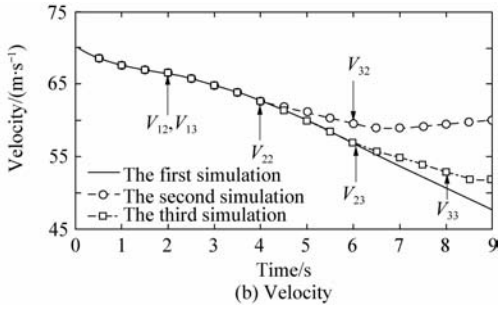
图 5 系统离散状态

Fig. 5 Discrete states of system

图 6 分别是 3 次仿真中系统连续变量(飞行高度与速度)的输出。



(a) Altitude



(b) Velocity

图 6 连续变量输出

Fig. 6 Output of continuous variables

第 1 次仿真中，$t=0$ s 时，高度 $z=300$ m，在 $z=270$ m 时飞机进入无风区，其后的应急操作全部失败，飞行高度与速度均急速下降。

第 2 次仿真中 0～4 s 与第 1 次仿真相同，第 4 s 和第 6 s 的手动油门以及手动俯仰角操作均成功。速度曲线经历拐点 V_{22} 和 V_{32}，速度下降减缓，$t=9$ s 时进入安全状态。高度曲线与之类似，在经历了代表两次成功应急操作的拐点 A_{22} 和 A_{32} 后，进入安全状态。

第 3 次仿真的速度和高度曲线变化趋势与第 2 次仿真类似，由于应急操作延迟，当飞行到 $t=9$ s 时，系统进入事故状态。

仿真结果反映了事故发展过程中系统的状态以及系统状态变量的变化行为，实现了系统中离散与连续特征的交互。

4 结 论

所提出的基于混合动态系统理论的事故过程建模方法，着眼于研究事故发展过程的离散与连续交互特性，主要结论如下：

(1) 将混合动态系统建模思想引入事故过程建模中，仿真模型用于实现事故过程机理研究。

(2) 实现了混合动态系统理论与事故过程特性的结合，以混合自动机实现了事故过程中连续与离散行为交互的建模，并在 Simulink/Stateflow 平台实现模型的开发，为明确事故过程的动态行为、制定应急措施提供了方法。

(3) 以案例演示方法的使用，验证了该建模方法的有效性。

参 考 文 献

[1] Hollnagel E. Understanding accidents—from root causes

to performance variability[C]// Proceedings of the 2002 IEEE 7th Conference on Human Factors and Power Plants: New Century, New Trends. Scottsdale Arizona, USA: Institute of Electrical and Electronics Engineers Inc., 2002: 1-6.

[2] Leveson N. A new accident model for engineering safer systems[J]. Safety Science, 2004, 42(4): 237-270.

[3] NASA. Probabilistic risk assessment procedures guide for NASA managers and practitioners[M]. Washington, D.C.: NASA, 2002.

[4] Hakata T. Seismic PSA method for multiple nuclear power plants in a site[J]. Reliability Engineering and System Safety, 2007, 92(7): 883-894.

[5] 罗鹏程. 基于Petri网的系统安全性建模与分析技术研究[D]. 长沙: 国防科学技术大学信息系统与管理学院, 2001.
Luo Pengcheng. A study on the modeling and analysis technique of system safety analysis based on Petri nets[D]. Changsha: College of Information System and Management, National University of Defense Technology, 2001. (in Chinese)

[6] 王蓓. 基于PFMEA与SIMULINK的应急预案仿真技术研究[D]. 北京: 北京航空航天大学可靠性与系统工程学院, 2011.
Wang Bei. Research on the simulation of emergency treatment based on PFMEA and SIMULINK[D]. Beijing: School of System Engineering of Engineering Technology, Beihang University, 2011. (in Chinese)

[7] Devooght J, Smidts C. Probabilistic dynamics as a tool for dynamic PSA[J]. Reliability Engineering and System Safety, 1996, 52(3): 185-196.

[8] 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 Armamentarii, 2009, 30(11): 1533-1539. (in Chinese)

[9] Labeau P E. A Monte Carlo estimation of the marginal distributions in a problem of probabilistic dynamics[J]. Reliability Engineering and System Safety, 1996, 52(3): 65-75.

[10] Cojazzi G. The DYLAM approach for the dynamic reliability analysis of systems[J]. Reliability Engineering and System Safety, 1996, 52(3): 279-296.

[11] Antsaklis P J, Stiver J A, Lemmon M D. Hybrid system modeling and autonomous control systems[R]. Lecture Notes in Computer Science: Hybrid Systems I. New York, USA: Springer-Verlag, 1993, 736: 366-392.

[12] Alur T, Courcoubetis C, Henzinger T A, et al. Hybrid automata, an algorithmic approach to the specification and verification of hybrid systems[R]. Lecture Notes in Computer Science: Hybrid Systems I. New York, USA: Springer-Verlag, 1993, 736: 209-229.

[13] Stiver J A, Antsaklis P J, Lemmon M D. Interface and controller design for hybrid control systems[R]. Lecture Notes in Computer Science: Hybrid Systems II. New York, USA: Springer-Verlag, 1995, 999: 462-492.

[14] Shi P, Zhao Y W, Cui Y J. Modeling and control of wheeled mobile robot based on hybrid automata[C]// 2010 Chinese Control and Decision Conference. Piscataway, USA: IEEE Computer Society, 2010: 3375-3379.

[15] Verma R, Vecchio D D. Continuous control of hybrid automata with imperfect mode information assuming separation between state estimation and control[C]// Proceedings of the 48th IEEE Conference on Decision and Control held jointly with 2009 28th Chinese Control Conference. Piscataway, USA: Institute of Electrical and Electronics Engineers Inc., 2009: 3175-3181.

[16] Mitra S, Wang Y, Lynch N, et al. Safety verification of model helicopter controller using hybrid input/output automata[R]. Lecture Notes in Computer Science: Hybrid Systems—Computation and Control, 2003, 2623: 343-358.

[17] Law A M, Kelton W D. Simulation modeling and analysis[M]. 3rd ed. New York: McGraw-Hill, 2000: 8-21.

[18] 林怡青, 毛宗源. 离散事件动态系统的结构[J]. 控制理论与应用, 2002, 19(5): 689-698.
Lin Yiqing, Mao Zongyuan. Structure of the DEDS[J]. Control Theory and Applications, 2002, 19(5): 689-698. (in Chinese)

[19] 戎梅, 赵廷弟, 李晓磊. 事故推演建模技术研究[J]. 航空学报, 2008, 29(6): 1563-1569.
Rong Mei, Zhao Tingdi, Li Xiaolei. Research on accident rehearsal modeling technique[J]. Acta Aeronautica et Astronautica Sinica, 2008, 29(6): 1563-1569. (in Chinese)

[20] 康立山, 曹宏庆, 陈毓屏. 动态系统的演化建模[J]. 计算机研究与发展, 1999, 36(8): 923-931.
Kang Lishian, Cao Hongqing, Chen Yuping. A hybrid evolutionary modeling algorithm for dynamic systems[J]. Journal of Computer Research and Development, 1999, 36(8): 923-931. (in Chinese)

[21] Agrawall A, Simon G, Karsai G. Semantic translation of Simulink/Stateflow models to hybrid automata using graph transformations[J]. Electronic Notes in Theoretical Computer Science, 2001, 109: 43-56.

[22] 张威. Stateflow逻辑系统建模[M]. 西安: 西安电子科技大学出版社, 2007: 56-124.
Zhang Wei. Stateflow logic system modeling[M]. Xi'an: Xidian University Publishing House, 2007: 56-124. (in

Chinese)
[23] 肖业伦. 大气扰动中的飞行原理[M]. 北京：国防工业出版社，1993：107-164.
Xiao Yelun. Flight principle in atmospheric disturbance [M]. Beijing: National Defense Industry Press, 1993: 107-164. (in Chinese)

作者简介：
王薇(1983—) 女，博士研究生。主要研究方向：安全性工程。
Tel：010-82317665
E-mail：wangwei@dse.buaa.edu.cn

赵廷弟(1965—) 男，博士，教授，博士生导师。主要研究方向：可靠性工程，安全性工程。
Tel：010-82316570
E-mail：ztd@buaa.edu.cn

Research on Accident Process Modeling Based on Hybrid Dynamic System Theory

WANG Wei , ZHAO Tingdi *

School of System Engineering of Engineering Technology, Beihang University, Beijing 100191, China

Abstract: An analysis of the accident characteristics in a system is proposed to research its accident process mechanism. The analysis indicates that there are hybrid characteristics which contain both discrete and continuous dynamic behaviors during an accident process. In view of the deficiency of simulating these hybrid characteristics with the current accident model, this paper presents a modeling method for accident processes based on hybrid system theory. The hybrid automata model of an accident process is provided, and the modeling and simulation is developed in the environment of Simulink/Stateflow. The combination of the system continuous mechanism with discrete state operation and their influence on each other can be achieved in this model. Then the simulation can provide the establishment of emergency treatment. Finally an example is discussed. The model simulates a dynamic process which starts at hazard and ends in accident or safety through emergency treatment. This example proves the validity of the proposed method.

Key words: accident; safety engineering; model; hybrid dynamic system; automata theory; Simulink

Received: 2011-03-08; **Revised**: 2011-04-25; **Accepted**: 2011-07-18; **Published online**: 2011-08-10 11∶18
URL: www.cnki.net/kcms/detail/11.1929.V.20110810.1118.003.html **DOI**: CNKI:11-1929/V.20110810.1118.003
* **Corresponding author.** Tel.: 010-82316570 E-mail: ztd@buaa.edu.cn