

文章编号:1000-8055(2011)03-0498-07

基于 SysML 的反推力系统安全性分析

尹树悦¹, 杨 云², 苗学问², 赵廷弟¹

(1. 北京航空航天大学 可靠性与系统工程学院, 北京 100191;

2. 中国人民解放军 空军装备研究院 总体所, 北京 100076)

摘 要: 通过应用系统工程建模工具 SysML(系统建模语言),对反推力系统的使用场景进行建模,分别建立起反推力系统的用例图和顺序图模型. 在使用场景模型的基础上,进一步应用 HAZOP(危险和可操作性)分析方法对使用场景进行危险分析,得到了反推力系统在使用中可能存在的危险状态,并提出了相应的安全性要求. 此方法应用表明,综合 SysML 和 HAZOP 的安全性分析是一种比传统的系统安全性分析更为有效的方法.

关 键 词: 反推力系统; 适航审定; 安全性分析; SysML(系统建模语言); 使用场景;
HAZOP(危险和可操作性)

中图分类号: V228.7⁺4

文献标识码: A

SysML-based safety analysis of thrust reverser

YIN Shu-yue¹, YANG Yun², MIAO Xue-wen², ZHAO Ting-di¹

(1. School of Reliability and System Engineering,

Beijing University of Aeronautics and Astronautics, Beijing 100191, China;

2. General Institute, Equipment Academy of Air Force,

The Chinese People's Liberation Army, Beijing 100076, China)

Abstract: System modeling language (SysML), a system engineering modeling tool, was employed to model operational scenario of thrust reverser according to SysML, and the case diagram model and sequence diagram model of thrust reverser were developed. Based on operational scenario model, hazard and operability (HAZOP) analysis technology was applied to analyze operational scenario hazards, and hazard conditions of thrust reverser in operation could be achieved by this method. Moreover, the corresponding safety requirements can be derived. The result of SysML-based safety analysis of thrust reverser shows that, integrating SysML and HAZOP is a more effective safety analysis method than traditional system safety analysis.

Key words: thrust reverser; airworthiness certification; safety analysis;
system modeling language (SysML); operational scenario;
hazard and operability (HAZOP)

大型飞机的反推力系统是飞机在地面减速着陆时为飞机提供减速功能的系统,尤其在湿滑跑道上降落时,反推力可以弥补机轮刹车效率的不足,提高飞机地面着陆时的安全性^[1].

运输类飞机适航标准 CCAR-25-R3 中的条款 25.933(a)(1)(ii)规定“仅预定在地面使用的发动机反推力系统必须设计成”——飞行中“反推力装置处于任何可能的位置时,飞机能继续安全

收稿日期:2010-01-21; 修订日期:2010-06-25

作者简介:尹树悦(1979—),男,河北张北人,博士生,研究方向:适航技术与管理,系统安全工程.

飞行和着陆”^[2]. 对于满足上述适航要求的符合性方法,现在即使是国外一些先进的飞机和发动机制造商也存在着直接表明符合性的困难,即设计上难以保证在空中意外打开反推力的情况下,飞机还能“继续安全飞行和着陆”,由于风险较大,一般也不会进行此类飞行试验. 通常的做法是采用“等效安全”的方法间接表明符合性^[3],即通过安全性分析来表明仅在地面使用的发动机反推力装置,在空中意外打开的概率为极不可能(不大于 10^{-9} /飞行小时). 另外,作为装在飞机上的一个分系统,反推力系统还必须满足 CCAR25. 1309 条款的要求,也即必须开展系统安全性分析来表明对此条款的符合性. 因此,在研制阶段对反推力系统开展安全性分析是适航审定和安全性设计工作的基础. 传统的系统安全性评估指南 SAE ARP4761 所提供的初步设计阶段的安全性分析方法——功能危险分析(FHA)是一种经验式的分析方法^[4],这种方法一方面难以完整地识别所分析对象的各种失效模式,另一方面也不能考虑具体的使用场景,将分析对象置于动态的使用过程中进行使用场景危险分析(实际上,动态的交互行为是引发危险的重要因素). 为此,本文提出应用国外最近几年开发的面向系统工程领域的系统建模工具 SysML(system modeling language,系统建模语言),结合 HAZOP(hazard and operability,危险和可操作性)分析这一安全性分析方法,对反推力系统进行形式化的安全性分析,为进一步明确反推力系统的安全性设计要求、以及安全性要求的确认和验证服务.

1 反推力系统工作原理

图1为一个典型的抓斗式反推力装置示意图^[5],其工作原理为:在空中正常工作情况下,反推力装置的两扇斗门完全关闭,锁机构将其上锁. 在反推力装置工作时,通过液压作动筒将两侧的斗门打开,由正推力气流施加给斗门形成的大于正推力气流 90° 角方向的气流即为反推力气流,由反推力气流产生与飞行方向相反的反推力,从而起到使飞机减速的目的.

反推力装置通过在座舱内设置的反推操纵杆进行操纵,通常,反推杆与正推力油门杆是集成于一体的. 反推杆和正推力油门杆之间有连锁机构,在进行正推力操纵时,反推杆被锁定,不能移动;在进行反推力操纵时,正推力油门杆被锁定在“慢车”位置,不能移动. 为防止反推力装置在空中意

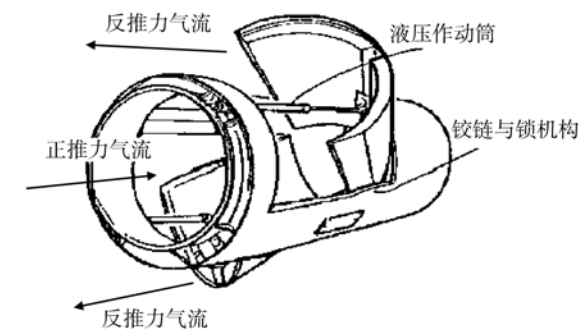


图1 反推力装置

Fig. 1 Thrust reverser system

外打开,一般在油门台上设置有电连锁机构,通过起落架系统传来的轮载或速度信号与电连锁机构进行关联,当收到解锁信号(轮载或速度)后解锁,方可进行反推力操纵. 另外,在座舱里还设置有反推力装置工作状态指示设备,以便飞行员及时判断反推力工作状态.

2 SysML 介绍

近几年软件开发领域流行的建模语言 UML(unified modeling language,统一建模语言)是面向对象的标准建模语言,其设计初衷是为软件开发提供一种标准建模规范,后来发展到也支持特定领域的建模. 为满足系统工程领域的需要,国际系统工程组织(International Council on Systems Engineering,简称 INCOSE)和对象管理组织(Object Management Group,简称 OMG)在对 UML 2.0 的子集进行重用和扩展的基础上,提出了一种新的系统建模语言——SysML,作为系统工程的标准建模语言. SysML 能够支持对各种复杂系统的详细说明、分析、设计、验证和确认,这些系统可能包括硬件、软件、信息、过程、人员和设施等^[6-7].

实际上,在软件安全性领域,人们已经在研究应用 UML 和各种传统的安全性分析方法相结合开展形式化的软件安全性分析^[5]. 但在系统安全性分析领域, SysML 出现之前 UML 还难以胜任包括硬件设备的复杂系统安全性分析. SysML 的出现为形式化的系统安全性分析提供了便利^[8].

3 基于 SysML 的反推力系统使用场景建模

本文从飞行员实施地面减速的使用和功能需求出发,应用 SysML 1.0 的用例图建立地面减速的用例模型,在此基础上再利用顺序图建立起反

推力系统的使用场景模型,以描述反推力系统在使用中的动态交互行为。

3.1 用例图

用例模型是从用户的视角来表达系统的使用和功能关系的模型。用例模型以图形化的方式来表示,用例图包括用例、操纵者和它们之间的关联关系。图2为飞行员实施地面减速的用例图。

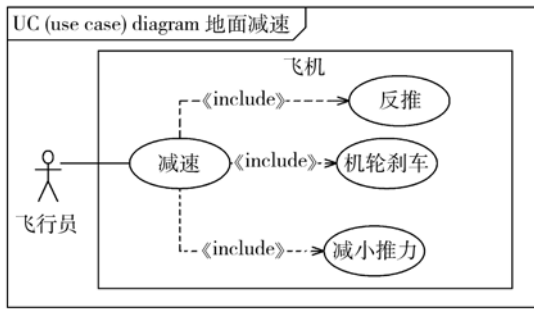


图2 地面减速用例图

Fig. 2 Use case diagram of decelerate on landing

图2表示飞行员在着陆过程中实施地面减速时与各功能间的交互,图中,椭圆形表示为各个用例,虚线加箭头表示基用例与其他用例之间的关系,“include”表示用例模型的包含关系。其中,飞机“减速”功能为基用例,“反推”、“机轮刹车”、“减小推力”用例与基用例形成包含关系,这3项功能为“地面减速”这一飞机级功能的子功能。飞行员

与“减速”用例之间的关联关系用实线表示,包含用例的系统(本文即指飞机)的边界用一个矩形来表示,系统的用例都置于矩形之内。

用例表示的是系统的功能,而功能又是由各种使用场景来实现的。“反推”用例的正常使用场景描述如表1,其中“前置状态”为进入场景前的状态,“后置状态”为场景结束后的状态^[5,9]。

表1 反推用例的场景

Table 1 Scenario of thrust reverse use case

反推用例场景:着陆减速	
前置状态	- 起落架已着陆 - 发动机处于工作状态
场景中的主要事件	- 飞行员将发动机正推力置于慢车状态 - 飞行员操纵执行反推力
后置状态	反推力被成功打开

3.2 顺序图

SysML通过顺序图对用例所包含的使用场景进行建模,以表达使用场景中按时间顺序发生的事件,以及事件中各对象之间的交互行为。根据图2中的反推用例模型和表1中对使用场景描述,得到以顺序图表示的正常情况下执行反推力操纵的使用场景模型,如图3所示。

图3中,顶端并列的各矩形表示使用场景中

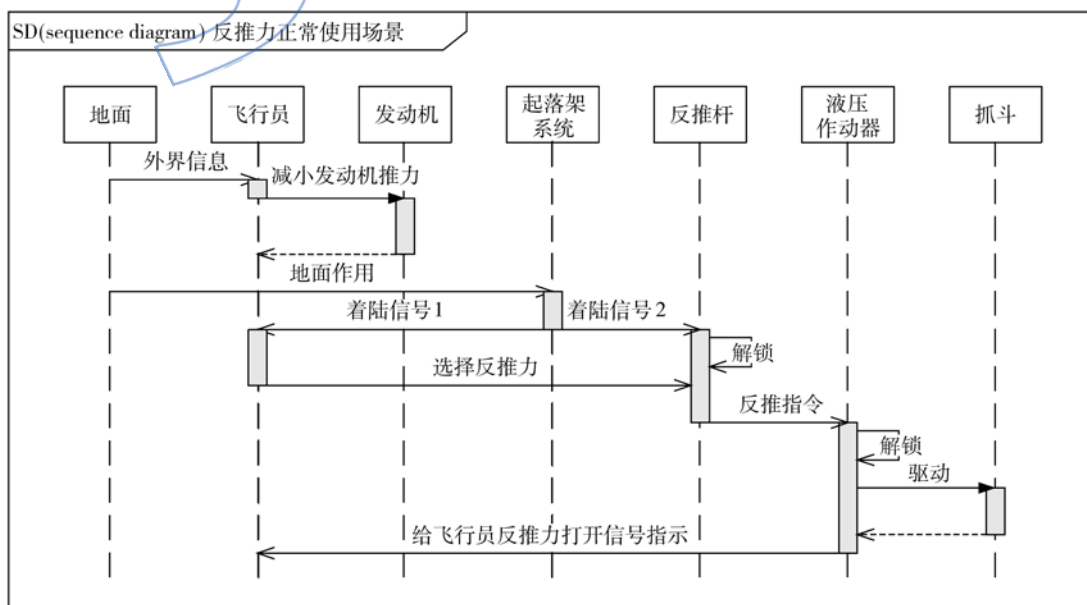


图3 反推力系统正常使用场景顺序图

Fig. 3 Sequence diagram of normal operational scenario of thrust reverser

相关的实体对象。实体对象下面垂直的虚线表示实体的“生命线”，即自上而下的时间推进。生命线上的窄矩形条被称为“激活”，激活表示该对象正在执行某个操作，激活矩形的长度表示激活持续的大致时间。带箭头的横向直线表示“消息”线，“消息”在这里是一个广义的词汇，既可表示信息或指令，又可表示动作或活动，因此，消息线的实际意义为信息/指令的传递或动作/活动的执行。其中，带实心箭头的实线表示同步消息，带两条线箭头的虚线表示同步消息的返回消息，带两条线箭头的实线表示异步消息。

4 应用 HAZOP 进行使用场景危险分析

4.1 HAZOP

HAZOP 方法最初是用来分析化学过程工业系统，后来被用于其他类型的系统以及软件等^[9]。HAZOP 是一种定性的技术，一般由不同专业人员组成的分析小组以会议的形式来开展工作。

HAZOP 一般在系统设计阶段的早期开展，从而能够通过分析影响设计，也可用来分析现有系统，以解决运行中的安全问题。

HAZOP 的基本指导思想是：任何偏离设计意图和正常运行行为的状态都可能引发危险，最终会导致事故^[10]。HAZOP 通过预先确定的引导词，与系统运行状态参数组合在一起表示成设计意图或运行状态的偏差，用来确定系统的危险，分析危险的原因、影响后果以及应采取的措施等。

传统的应用于化学过程工业的 HAZOP 方法设定有 7 个基本引导词^[11]，如表 2 所示。

另外，在进行其他类型对象的分析时，还有可能用到以下的一些补充引导词，见表 3。

在分析具体对象时，将所有引导词与所有具体要素相结合会产生一个偏差矩阵，在实际中，不同的参数或特性要素不可能全部都会产生所有引导词所导出的偏差模式，因此，偏差矩阵中的内容有些有意义，有些则没有实际意义，这就要确定矩阵中哪些偏差需要分析，哪些不需要。

表 2 基本引导词
Table 2 Basic guide-words

引导词	含义	说明
无/否	对设计意图的否定	完全没有达到设计或运行要求，也没有发生其他事件
较多	数量增加	比标准值在量上增加了(定量)
较少	数量减少	比标准值在量上减少了(定量)
以及/伴随	质的增加	完成既定要求的同时伴有多余事件发生(定性)
部分	质的减少	部分达到设计或运行要求(定性)
相反	设计意图逻辑上的对立	出现与设计或操作要求相反的事件
异常	完全代替	被与设计意图不同的事物代替，即设计意图没有实现，而发生了完全不同的其他事件

表 3 补充引导词
Table 3 Additional guide-words

引导词	含义
早/晚	事件发生的时间偏离了设计意图
之前/之后	事件序列与设计意图不相符
快/慢	事件持续的时间偏离了设计意图

4.2 针对 SysML 模型的 HAZOP 分析程序

在应用 SysML 的用例图和顺序图建立起反推力系统的功能和使用场景模型后，就可以利用 HAZOP 方法对使用场景进行危险分析。开展

HAZOP 分析的前提是确定所分析对象的要素，并确定相应的引导词，以导出偏差模式，从而识别出危险。具体分析程序的步骤如下：

- 1) 根据模型特点确定 HAZOP 分析的对象要素；
- 2) 根据要素特点确定相应的引导词；
- 3) 综合要素和引导词导出偏差；
- 4) 分析偏差造成的危险；
- 5) 确定危险的可能原因和后果；
- 6) 提出安全性要求或建议措施。

4.3 HAZOP 对顺序图使用场景的分析

应用 HAZOP 分析顺序图所建立的使用场

景模型,可以处理系统使用场景中复杂动态交互行为带来的危险.在对顺序图模型进行 HAZOP 分析时需要确定分析的要素.本文将顺序图中的“消息”作为 HAZOP 分析的要素,消息要素具体可细分为 3 种属性,分别为消息的时间属性、消息的目标属性和消息的状态属性^[12].根据消息要素 3 类属性的特点,可分别确定出 HAZOP 分析相应的引导词,如表 4、表 5 和表 6 所示.

表 4 针对消息时间属性的引导词

Table 4 Guide-words for time attribute of message

引导词	说明
无	在规定的时间无消息发送
伴随	消息在正确的时间发送也在无关的时间发送
早	消息早于规定的时间发送
晚	消息晚于规定的时间发送
之前	消息发送于规定的事件序列之前
之后	消息发送于规定的事件序列之后
快	消息发送持续时间变短
慢	消息发送持续时间变长
异常	消息在错误的时间发送

以上的引导词是一个全集,在针对具体的消息及其属性进行分析时,根据消息要素的特点可进行适当的取舍,去掉一些无意义的引导词.

表 5 针对消息目标属性的引导词

Table 5 Guide-words for destination attribute of message

引导词	说明
无	消息没有发送到指定的目标
较多	消息发送给比规定多的目标
较少	消息发送给比规定少的目标
伴随	消息发送给正确的目标也发送给无关的目标
相反	消息源和目标发生了颠倒
异常	消息发送给错误的目标

表 6 针对消息状态属性的引导词

Table 6 Guide-words for state attribute of message

引导词	说明
无	消息在传递中完全丢失
较多	消息的内容多于规定的量
较少	消息的内容少于规定的量
伴随	传递了多余的消息内容
部分	只实现了部分消息的传递
相反	消息传递了相反的内容
异常	消息传递了异常的内容

根据前面确定的分析程序和引导词,下面针对由顺序图建立的反推力使用场景模型,以对“着陆信号 2”和“反推指令”这两个消息的分析为例给出具体的 HAZOP 分析过程,如表 7、表 8 和表 9 所示.

表 7 消息时间属性的 HAZOP 分析

Table 7 HAZOP study on time attribute of message

序号	要素	引导词	偏差	危险	可能的原因	影响后果	安全性要求/建议措施
1	着陆信号 2	无	飞机着陆后没有给反推杆发送解锁信号	着陆时反推力打不开	传感器故障	可能导致飞机高速冲出跑道	传感器采取冗余措施
		早	飞机着陆前就给反推杆发送了解锁信号	可能在着陆前打开反推(考虑与其他情况的组合)	传感器故障	飞行员需应急处置,增加了工作负担	增加信息源和传感器,综合判断飞机着陆状态
		晚	飞机着陆后一段时间才给反推杆发送解锁信号	飞机不能及时减速	传感器故障	增加了飞行员工作负担,飞机有可能会冲出跑道	增加信息源和传感器,综合判断飞机着陆状态
		异常	飞机在空中就给反推杆发送解锁信号	可能在空中打开反推力(考虑与其他情况的组合)	传感器故障	推力突变,可能导致灾难性后果	增加信息源和传感器,综合判断飞机着陆状态

续表 7

序号	要素	引导词	偏差	危险	可能的原因	影响后果	安全性要求/ 建议措施
2	反推指令	无	没有根据飞行员的操作给液压作动器发送反推指令	着陆时反推力打不开	反推操纵系统故障	可能导致飞机高速冲出跑道	考虑操纵系统采取冗余措施
		异常	飞机在空中就给液压作动器发送反推指令	空中打开反推力	软件运行错误	推力突变,可能导致灾难性后果	加强研制中软件测试和过程控制

表 8 消息目标属性的 HAZOP 分析
Table 8 HAZOP study on destination attribute of message

序号	要素	引导词	偏差	危险	可能的原因	影响后果	安全性要求/ 建议措施
1	着陆信号 2	无	解锁信号没有发送到反推杆	着陆时反推力打不开	信号传输通路失效	可能导致飞机高速冲出跑道	提高信号传输的可靠性
2	反推指令	无	反推指令没有发到液压作动器	着陆时反推力打不开	信号传输通路失效	可能导致飞机高速冲出跑道	提高信号传输的可靠性

表 9 消息状态属性的 HAZOP 分析
Table 9 HAZOP study on state attribute of message

序号	要素	引导词	偏差	危险	可能的原因	影响后果	安全性要求/ 建议措施
1	着陆信号 2	无	飞机着陆后反推杆解锁信号在发送过程中丢失	着陆时反推力打不开	信号传输通路失效;电磁干扰	可能导致飞机高速冲出跑道	提高信号传输的可靠性;采取防电磁干扰措施
		伴随	飞机着陆后反推杆解锁信号被干扰	着陆时反推力打不开	电磁干扰	可能导致飞机高速冲出跑道	采取防电磁干扰措施
		部分	飞机着陆后反推杆解锁信号部分丢失	着陆时反推力打不开	电磁干扰	可能导致飞机高速冲出跑道	采取防电磁干扰措施
2	反推指令	无	反推指令在发送过程中丢失	着陆时反推力打不开	信号传输通路失效;电磁干扰	可能导致飞机高速冲出跑道	提高信号传输的可靠性;采取防电磁干扰措施
		相反	打开指令变为关闭指令	着陆时反推力打不开	软件运行错误	可能导致飞机高速冲出跑道	加强研制中软件测试和过程控制

由于篇幅所限,本文只列举了针对两个消息要素的 HAZOP 分析例子,如果将使用场景中所有的消息要素都加以分析,可以得到一系列的风险分析结果,最后可将所有分析得到的安全性要

求或建议措施综合,最终获得反推力系统的安全性设计要求.在进入详细设计阶段、获得足够的设计信息后,可以将 HAZOP 分析得到的危险状态作为顶事件开展 FTA(故障树分析)以及设备和部件的 FMEA(故障模式和影响分析)工作,以支持定量的安全性要求分配和适航符合性验证.

5 结 论

SysML 作为系统工程领域的一个重要建模工具,为基于模型的系统安全性分析提供了有效途径.本文应用 SysML 对反推力系统进行了用例和使用场景的建模,并针对 SysML 顺序图模型的特点对传统的 HAZOP 引导词及其含义进行了扩展,进一步为 SysML 与 HAZOP 的综合应用提供了便利.在使用场景建模的基础上结合 HAZOP 方法开展了反推力系统使用场景的危险分析,由分析的实例可以看到,基于 SysML 顺序图模型的 HAZOP 分析能很好地处理系统使用过程中各种动态的交互行为带来的危险.将顺序图中的消息划分为不同属性,并分别针对同一消息的不同的属性应用不同的引导词开展 HAZOP 分析,进一步细化了使用场景中各种失效模式,可以推理得到传统的 FHA 等方法难以识别的危险,这有利于系统安全性设计的改进和安全性水平的提升.

参考文献:

- [1] 靳宝林,邢伟红,刘殿春.飞机/发动机推进系统反推力装置[J].航空发动机,2004,30(4):48-57.
JIN Baolin, XING Weihong, LIU Dianchun. Thrust reversers of aircraft/engine propulsion system[J]. Aeroengine, 2004, 30(4): 48-57. (in Chinese)
- [2] 中国民用航空总局. CCAR-25-R3 运输类飞机适航标准[S].北京:中国民用航空总局,2005.
Civil Aviation Administration of China. CCAR-25-R3 Airworthiness standards: transport category airplanes[S]. Beijing: Civil Aviation Administration of China, 2005. (in Chinese)
- [3] Neil D S. Equivalent level of safety finding for the airbus model A380-800 (FAA project number CP101)[EB/OL]. [2010-01-09]. [Http://rgl.faa.gov/Regulatory_and_Guidance_Library/rg.ELOS.nsf/0/c7d650487a6d2575862574cd006a39cd/\\$FILE/CP101-P-02.pdf](http://rgl.faa.gov/Regulatory_and_Guidance_Library/rg.ELOS.nsf/0/c7d650487a6d2575862574cd006a39cd/$FILE/CP101-P-02.pdf).
- [4] Society of Automotive Engineers. SAE ARP4761 Guidelines and methods for conducting the safety assessment process on airborne systems and equipments[S]. US: The Engineering Society for Advancing Mobility Land Sea Air and Space, 1996.
- [5] Iwu F, Galloway A, McDermid J, et al. Integrating safety and formal analyses using UML and PFS[J]. Reliability Engineering and System Safety, 2007, 92(2): 156-170.
- [6] 蒋彩云,王维平,李群. SysML: 一种新的系统建模语言[J]. 系统仿真学报, 2006, 18(6): 1483-1492.
JIANG Caiyun, WANG Weiping, LI Qun. SysML: a new systems modeling language[J]. Journal of System Simulation, 2006, 18(6): 1483-1492. (in Chinese)
- [7] Object Management Group. OMG systems modeling language(OMG SysML), V1.0[EB/OL]. [2009-12-30]. [Http://www.omg.org/spec/SysML/1.0/PDF](http://www.omg.org/spec/SysML/1.0/PDF).
- [8] David P, Idasiak V, Kratz F. Reliability study of complex physical systems using SysML[J]. Reliability Engineering and System Safety, 2010, 95(4): 431-450.
- [9] Allenby K, Kelly T. Deriving safety requirements using scenarios[C]//Proceeding of the Fifth IEEE International Symposium on Requirements Engineering. Silver Spring, MD: IEEE Computer Society Press, 2001: 228-235.
- [10] MU Fangping. Multivariate statistical process monitoring and its integration with HAZOP analysis for abnormal event management[D]. West Lafayette, US: Purdue University, 2003.
- [11] 赵文芳,姜春明,姜巍巍,等. HAZOP 分析核心技术[J]. 安全健康和环境, 2005, 5(3): 1-3.
ZHAO Wenfang, JIANG Chunming, JIANG Weiwei, et al. The core technology of HAZOP analysis[J]. Safety, Health and Environment, 2005, 5(3): 1-3. (in Chinese)
- [12] Lano K, Clark D, Androutsopoulos K. Safety and security analysis of object-oriented models[J]. Lecture Notes in Computer Science, 2002, 2434: 82-93.