【后勤保障与装备管理】 doi: 10.11809/scbgxb2017.09.030

基于 BDD 的安全注射系统共因失效分析方法

戚加军,赵新文,张永发,郭海宽

(海军工程大学 核能科学与工程系,武汉 430033)

摘要:针对用传统的 PSA 方法分析含有共因失效系统的可靠性时计算量大、耗时长,提出了利用二元决策图(BDD)与共因失效隐式分析相结合的方法对系统可靠性进行计算。建立系统故障树并转化为 BDD 图得到系统可靠度的不交化表达式,结合共因失效隐式分析,将该式转化成含共因失效的可靠度表达式,并以安全注射系统为例进行可靠度分析计算。结果表明:BDD 图与共因失效隐式分析相结合的方法对含有共因失效的复杂系统进行可靠性分析时简便有效,计算结果更符合实际情况。

关键词:二元决策图;故障树;共因失效;隐式分析

本文引用格式:戚加军,赵新文,张永发,等. 基于 BDD 的安全注射系统共因失效分析方法[J]. 兵器装备工程学报,2017(9):143 - 147.

Citation format:QI Jiajun, ZHAO Xinwen, ZHANG Yongfa, et al. Common Cause Failure Analysis Method of Safety Injection System Based on BDD[J]. Journal of Ordnance Equipment Engineering,2017(9):143 - 147.

中图分类号:TL387 **文献标识码**:A **文章编号**:2096 - 2304(2017)09 - 0143 - 05

Common Cause Failure Analysis Method of Safety Injection System Based on BDD

QI Jia-jun, ZHAO Xinwen, ZHANG Yongfa, GUO Haikuan

(Department of Nuclear Science and Technology, Naval University of Engineering, Wuhan 430033, China)

Abstract: The traditional PSA method is used to analyze the reliability of the system with common cause failure spend large amount of calculation and time. In this paper, we propose a method of combining binary decision diagram (BDD) with common cause failure(CCF) implicit analysis to calculate the reliability of the system. The system fault tree is established and transformed into the BDD to get the disjoint expression of system reliability, combined with CCF implicit analysis to transform it into a reliability expression with CCF. In this paper, an example is given to analyze the reliability of safety injection system. Results show that it is simple and effective to analyze the reliability of complex systems with CCF by the combination of BDD diagram and CCF implicit analysis, the calculation results are more in line with the actual situation.

Key words: binary decision diagram; fault tree; common cause failure; implicit analysis

共因失效是系统受环境、人因、构造等共同的原因导致系统内的多个部件同时失效[1,2]。在概率安全评价(PSA)中部件间的共因失效是研究的重要部分,也是研究的难点。目前大型的复杂系统为了提高系统可靠性会对核心设备和部件做冗余设计,但在实际运行过程发现系统可靠性并没有大幅提高,出现这种情况是由于系统中共因失效的影响导致系统的可靠度降低[3]。目前分析共因失效的模型主要有 α 因子模型、β 因子模型、MGL 模型(多希腊字母),分析系统总

收稿日期:2017 - 05 - 18;**修回日期**:2017 - 05 - 30

作者简介:戚加军(1992—),男,硕士研究生,主要从事核科学与技术研究。

失效概率时一般要分别考虑系统部件单独失效和部件间共因失效对整个系统可靠性的影响[4]。传统的 PSA 方法计算系统失效概率时底事件的数量巨大,求出的割集和路集多,对割集和路集进行不交化处理时难度大且过程繁琐,将故障树转化为 BDD 图可以利用计算机直接求故障树的不交化路集[5-7]。参照系统运行逻辑图,结合系统的可靠度不交化表达式分析系统的可靠度,利用共因失效的隐式分析方法[8]可对包含共因失效的系统可靠度进行计算求解。结合某船用核动力装置的安全注射系统,分析安注系统工作原理和逻辑[9-10],对安注系统的含共因失效时的系统可靠度进行定量计算并与不考虑共因失效时系统可靠度进行对比。本文提出的方法大大简化了复杂系统含共因失效的可靠度计算量,计算分析结果符合实际。

1 二元决策图求解方法

通过分析系统的功能原理和结构组成情况可建立系统故障树。将系统故障树用递归运算法转化为二元决策图形式[3],可直接计算出系统可靠度的不交化表达式。常用的故障树向二元决策图转化方法有 ite 运算(If-Then-Else)和成分组合法,本文介绍 ite 运算方法向 BDD 转化,ite 运算的基本表达式为

$$f = \mathrm{ite}(X,A,B) \tag{1}$$

基本事件 X 是父节点,A 和 B 为故障树左右子节点。如果事件 X 发生则其发生概率为 A,否则事件 X 不发生概率的为 B。其概率表达式为:

$$f = \mathrm{ite}(X,A,B) = X \cdot A + \bar{X} \cdot B \tag{2}$$

将故障树底事件进行规范化处理,使故障树只含有与、或、非 3 种逻辑门,若中间事件含有非门用 DeMorgan(德摩根)定律处理使中间事件仅含有与门和或门,底事件可以有非门。

对同一个故障树,底事件的指标顺序对 BDD 图的复杂程度有很重要的影响。底事件指标顺序选取的合适可以大大减少故障树向 BDD 图转化的工作量,如何确定底事件的指标(index)顺序是 BDD 研究的重要课题。本文用文献[6]中推荐的方法对底事件进行指标排序,即:① 靠近故障树顶层的底事件在指标顺序上要优先考虑。② 故障树中反复出现多次的底事件优先考虑。③ 相邻基本事件在指标排序中也要相近。

定好底事件指标顺序后,用 ite 运算将编码完成后的底事件进行置换,根据底事件的优先顺序来构造 BDD 图形。运算过程中用到故障树逻辑门中的布尔规则。

假设 f 和 g 分别为故障树中的节点,$f = \mathrm{ite}(x_1,p_1,q_1)$,$g = \mathrm{ite}(x_2,p_2,q_2)$,$x_1$ 和 x_2 代表底事件,p_1 和 p_2 分别代表底事件 x_1,x_2 发生概率,q_1,q_2 代表底事件 x_1,x_2 不发生的概率。

若 $\mathrm{index}(x_1) > \mathrm{index}(x_2)$,则:$f\langle \mathrm{op}\rangle g = \mathrm{ite}(x_1,p_1\langle \mathrm{op}\rangle g, q_1\langle \mathrm{op}\rangle g)$。

若 $\mathrm{index}(x_1) = \mathrm{index}(x_2)$,则:$f\langle \mathrm{op}\rangle g = {}_i te(x_1,p_1\langle \mathrm{op}\rangle p_2, q_1\langle \mathrm{op}\rangle g_2)$。

其中〈op〉分别代表故障树逻辑运算中的与门(AND)和或门(OR)。

2 安全注射系统逻辑框图

压水堆的安全注射系统通过压力传感器检测一回路冷却剂压力变化判断是否发生冷却剂丧失事故(LOCA)。安全注射系统有补水,安注和再热循环 3 大功能,以保证一回路冷却剂的压力和装量保持稳定,确保堆芯不会裸露和烧毁。反应堆的安全注射系统具有明显的时序性和阶段性[11],系统的成功准则是保证反应堆不发生堆芯融化事故。在反应堆冷却剂系统发生承压边界破损导致一回路冷却剂压力降低时投入安全注射系统。该系统分为高压安注、低压安注、再热循环 3 部分组成,分别在冷却剂系统不同的压力下启动。

安全注射系统在反应堆发生冷却剂泄漏事故时及时向一回路冲水,满足堆芯的换热需求,保证堆芯被淹没不发生熔化等严重事故。安全注射系统主要由安注水源,安注泵,滤网,换热器以及相应的管道和阀门组成。安全注射系统根据一回路冷却剂系统的压力变化执行不同的动作,具有明显的阶段性[6]。

以某型船用反应堆安全注射系统为例,假设该反应堆在正常工作状态下系统内各个阀门和水泵均处于关闭状态,其他系统和部件的可靠性为 1,其工作逻辑框图如图 1 所示。为简化系统,本文暂不考虑安注系统的喷淋功能。反应堆在正常运行时在靠近堆芯入口段出现破口,发生冷却剂丧失事故,此时安注系统的响应过程分为如下 4 个阶段。

阶段 1($0 \sim t_1$):判断破口位置和大小,隔离环路。破口出现后,冷却剂丧失使一回路压力下降,当稳压器压力 x 下降至压力 P_1 时安全注射系统启动。开启控制阀 1 和控制阀 4,水源 1 启用,向水泵 1 供水,开启控制阀 3,冷却水通过控制阀 7 和控制阀 8 注入堆芯。

阶段 2($t_1 \sim t_2$):成功隔离破口环路,关闭控制阀 7(控制阀 8),冷却水从靠近堆芯的控制阀 7(控制阀 8)注入反应堆芯。

阶段 3($t_2 \sim t_3$):稳压器压力 x 继续下降,当 x 的值降至压力 p_2 时($P_1 > P_2$),关闭控制阀 4,开启控制阀 5 启动水源 2 向水泵 1 供水;开启控制阀 2 水源 1 向水泵 2 供水,两股水流同时通过控制阀 3 流向控制阀 7 和控制阀 8 注入堆芯。

阶段 4($t_3 \sim t_4$):水源 1 和水源 2 水量不足停止供水,关闭控制阀 1、2、3、4、5 和水泵 1,开启控制阀 9 启动水源 3,开启控制阀 6,水泵 2 从水源 3 处吸水,经过换热器降温后通过控制阀 7、8 进入堆芯。

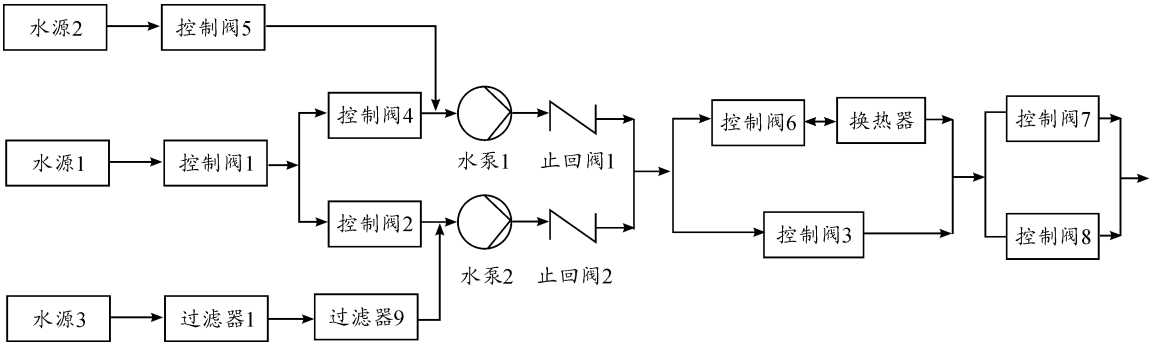

图 1　安全注射系统工作逻辑框图

3　故障树建模及二元决策图转化

安注系统执行功能时水源 1 既可以向水泵 1 和水泵 2 注水,水源 2 向水泵 1 注水。安注系统注射水都需要经过控制阀 7、8 进入堆芯,高压安注水和低压安注水要经过控制阀 3,因此水源 1,控制阀 3 和控制阀 7、8 的可靠性对整个安注系统的可靠性有较大影响。分析安注系统功能和失效原理,建立如图 2 所示的故障树。

从图 2 可看出故障树较大,难以用传统方法计算共因失效。由于故障树的底事件数目多,不同的指标排序会对生成的 BDD 图的中间计算过程有较大影响。本文利用文献[6]中介绍的方法对故障树底事件进行排序,其指标排列顺序为:

$$x_5 > x_{12} > x_{16} > x_{11} > x_1 > x_6 > x_7 > x_{13} > x_{14} > x_{15} > x_{10} > x_4 > x_2 > x_3 > x_{12} > x_8 > x_9$$

根据图 2 故障树,由布尔法则计算顶事件 A,安注系统的失效概率为:

$$A = B_1 + B_2 + B_3 + B_4$$

各中间事件发生失效的概率分别为:

$$B_1 = C_1 + C_2 = x_1 + D_1 + x_5 \cdot x_6 = x_1 + x_2 + x_3 + x_4 + x_5 + x_6$$

$$B_2 = x_7 + x_8 + x_9 + x_{10} + x_4 + x_5$$

$$B_3 = x_{12} + x_{13} + x_{14} + x_{15} + x_{10}$$

$$B_4 = x_{16} \cdot x_{11}$$

将图 2 故障树用递归法,ite 运算转化为 BDD 二元决策图。故障树顶事件 A 可以用 ite 形式表示为:

A = ite(x_5,1,ite(x_{12},1,ite(x_{16},ite(x_{16},ite(x_{11},1,ite(x_1,1,ite(x_6,1,ite(x_7,1,ite(x_{13},1,ite(x_{14},1,ite(x_{15},1,ite(x_{10},1,ite(x_4,1,ite(x_3,1,ite(x_8,1,ite(x_9,1,0),ite(x_{15},1,ite(x_{10},1,ite(x_4,1,ite(x_3,1,ite(x_8,1,ite(x_9,1,0))))))))))))))))),ite(x_{15},1,ite(x_{10},1,ite(x_4,1,ite(x_3,1,ite(x_8,1,ite(x_9,1,0)),ite(x_{15},1,ite(x_{10},1,ite(x_4,1,ite(x_3,1,ite(x_8,1,ite(x_9,1,0))))))))))))))))))))))。

将所有的门事件用 ite 运算进行置换,使故障树的基本事件成为 BDD 图中的一个节点,得到相应的二元决策图如图 3 所示。

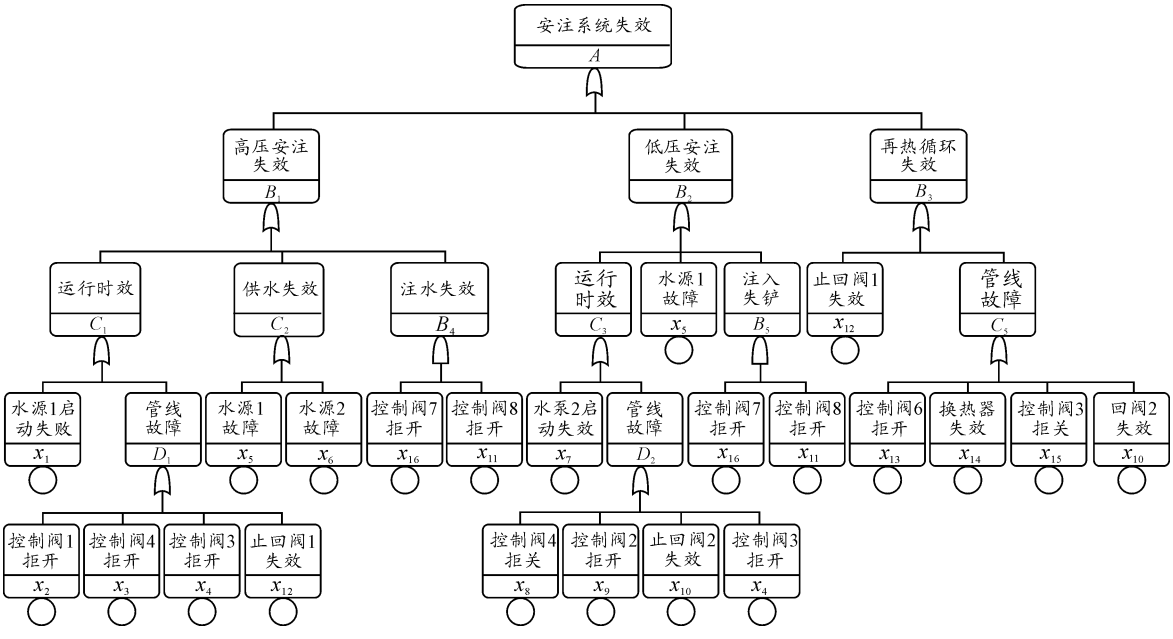

图 2　安注系统失效故障树

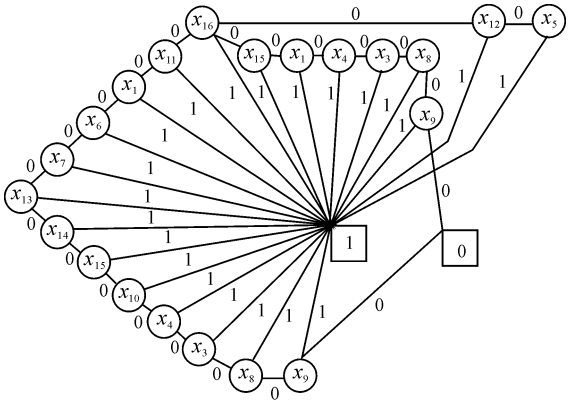

图 3 故障树转化为 BDD 图

通过 BDD 图容易得到系统的不交化路集,从节点 x_5 出发的所有至节点 0 的支路节点。组合都表示为能使系统正常运行的基本事件组合。

4 安注系统共因失效分析

由安注系统工作原理可看出,系统内阀门数量较多,在不同阶段系统切换功能时,会频繁涉及到阀门的开启和关闭,阀门的可靠性对整个系统可靠性的影响重大。系统内某个阀门的失效直接影响到安注系统功能的执行,一个阀门失效后会引起其他阀门受到冷却剂冲击发生共因失效,因此以图 1 所示安注系统所有的阀门为同一共因组,其他部件的失效与阀门失效相互独立。存在共因失效时系统同一共因组部件承受到共因冲击,其他部件的失效相互独立,具有相同的概率分布且含有多种失效模式。

不考虑共因失效时系统内某一部件正常的概率为 p。在隐式分析方法中,共因组部件总数目为 n,λ_i 表示共因组内指定的 i 个单元同时或者在短时间内相继发生故障的概率,共因组中一个指定单元正常的概率为 $p_n^1(t)$

$$p_n^1(t) = \exp\left(-\sum_{i=1}^{n} c_{n-1}^{i-1}\lambda_i t\right) \tag{1}$$

在共因失效组里 n 个部件中指定 m 个部件正常的概率为

$$p_n^m(t) = \prod_{k=n-m+1}^{n} p_k^1(t) \tag{2}$$

联立式(1)和式(2)得到共因组中所有部件正常运行的概率为

$$p_n^n = \exp\left(-\sum_{j=1}^{n} c_n^j\lambda_i t\right) \tag{3}$$

通过图 3 的二元决策图,在不考虑共因失效情况下安注系统的可靠度表达式为

$$\begin{aligned} R = {} & x_5 \cdot x_2 \cdot x_{16} \cdot x_{15} \cdot x_{10} \cdot x_4 \cdot x_3 \cdot x_2 \cdot x_8 \cdot x_9 \cdot \\ & x_5 \cdot x_{12} \cdot x_{16} \cdot (\bar{x}_{11} \cdot x_1 \cdot x_6 \cdot x_7 \cdot x_{13} \cdot x_{14} \cdot \\ & x_{15} \cdot x_{10} \cdot x_4 \cdot x_3 \cdot x_2 \cdot x_8 \cdot x_9 \end{aligned} \tag{4}$$

由于假设将安注系统原理图中所有的阀门作为处于同一共因失效组,其他部件的失效受到的冲击是相互独立的泊松过程。从安注系统原理图中看出系统内有控制阀和止回阀两种阀门,查阅相关失效数据,控制阀失效概率明显高于止回阀,因此进行共因失效时要分开考虑。设控制阀正常工作的概率为 $p(t)$,止回阀正常工作的概率为 $f(t)$。在不考虑共因失效情况下系统的可靠度为

$$\begin{aligned} R_s = {} & x_5 \cdot f(t) \cdot p^8(t) + f^2(t) \cdot x_5 \cdot \bar{x}_{11} \cdot x_1 \cdot \\ & x_6 \cdot x_7 \cdot x_{14} \cdot p^8(t) \end{aligned} \tag{5}$$

在考虑阀门间共因失效时安注系统的可靠度为

$$\begin{aligned} R_c = {} & f_2^1(t) \cdot x_5 \cdot p_8^8(t) + f_2^2(t) \cdot x_5 \cdot \bar{x}_{11} \cdot \\ & x_1 \cdot x_6 \cdot x_7 \cdot x_{14} \cdot p_8^8(t) \end{aligned} \tag{6}$$

本文采用的数据来源于中国核电厂设备可靠性数据报告(2015 版),其中安注系统的主要设备的失效数据如表 1 所示。

表 1 安注系统设备失效数据

编号	设备名称	失效概率/h
1	水源 1、2、3	3.19E-08
2	安注泵 1、2	2.11E-05
3	止回阀	4.99E-05
4	换热器	6.45E-07
6	控制阀	1.25E-04

假设控制阀失效率 $\lambda_1 = 1.25\text{E}-04$, $\lambda_2 = 1.25\text{E}-05$, $\lambda_3 = 1.25\text{E}-06$ 直至 $\lambda_8 = 1.25\text{E}-11$,止回阀失效率 $\alpha_1 = 4.99\text{E}-05$, $\alpha_2 = 4.99\text{E}-05$。由于设备同时失效的数据还没有文献可以查阅参考故先假设 λ 的值。

表 1 中的数据带入表达式(5),得到在不考虑共因失效时系统可靠度计算结果为

$$\begin{aligned} R_s = {} & \exp(-1.050\times10^{-3t}) + \exp(-1.120\times10^{-3t}) - \\ & \exp(-1.246\times10^{-3t}) \end{aligned} \tag{7}$$

将数据带入表达式(6),同理可得在考虑共因失效时系统的可靠度计算结果为

$$\begin{aligned} R_c = {} & \exp(-1.483\times10^{-3t}) + \exp(-1.570\times10^{-3t}) - \\ & \exp(-1.695\times10^{-3t}) \end{aligned} \tag{8}$$

安注系统在不考虑共因失效时的不可靠度为 Q_s,$Q_s(t) = 1 - R_s(t)$。

安注系统在考虑共因失效时的不可靠度为 Q_c,$Q_c(t) = 1 - R_c(t)$。

在 Python 软件上画出函数 Q_s 和 Q_c 随时间变化的曲线图像如图 4 所示,考虑到实际情况安注系统的投入时间一般不会超过 50 h,所以时间 t 的取值范围为 0 ~ 50 h。

由图 4 可看出安注系统的不可靠度随时间的增加越来越大,考虑共因失效时安注系统的不可靠度变化更明显。在第 50 小时 Q_c 的值是 Q_c 值的 1.35 倍。系统投入时间越长两者相差越大。

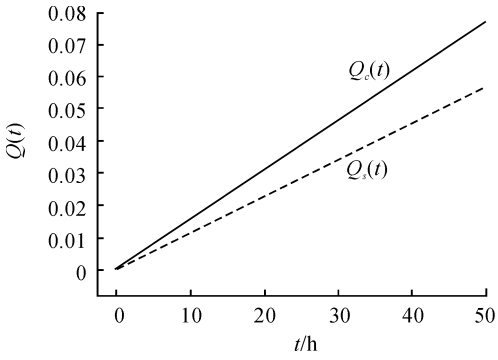

图 4 Q_s 和 Q_c 随时间变化曲线

5 结论

1) 由于系统设备间存在共因失效的相互影响,导致系统可靠度低于设备相互独立时系统的可靠度。

2) 将复杂系统的大故障树转化为 BDD 图再进行分析可以节省时间和计算量,省略了对大故障树的最小割集和最小路集的不交化求解,利用计算机可直接计算。

3) 对复杂系统同一类型的设备归为同一共因组,利用共因失效的隐式分析可计算系统的可靠度,计算结果可靠,更符合实际情况。

4) 客服传统共因失效模型(α 和 β 模型)的局限性,可对两个或多个设备间相互影响下的情况进行共因失效分析计算。

参考文献:

[1] ANDREW O'CONNOR, ALI MOSLEH. A general cause based methodology for analysis of common cause and dependent failures in system risk and reliability assessments [J]. Reliability Engineering and System Safety, 2016, 145: 341 – 350.

[2] 张国军,朱俊,吴军,朱海平. 基于 BDD 的考虑共因失效的故障树可靠性分析[J]. 华中科技大学学报(自然科学版),2007(9):1 – 4.

[3] 贺理,陈杰,周继翔,等. 共因失效对平均失效概率计算结果的影响分析[J]. 核动力工程,2014(6):158 – 161.

[4] 朱春丽,王浩,杨金丽. 基于共因失效的系统可靠性分析[J]. 石油化工自动化,2016(4):10 – 12.

[5] AKERS S B. Binary Transaction on Computer, decision diagrams[J]. IEEE1978, 27:509 – 516.

[6] 闵苹,童节娟,奚树人. 利用二元决策图求解故障树的基本事件排序[J]. 清华大学学报(自然科学版),2005(12):1646 – 1649.

[7] BARTLETT L M, ANDREWS J D. Efficient basic event ordering schemes for fault tree analysis[J]. Qual Reliab Engng Int, 1999(2):95 – 101.

[8] 金星,洪延姬,杜红梅. 共因失效系统的可靠性分析方法[M]. 北京:国防工业出版社,2008.

[9] 时劲科,陈力生,陈玲,等. 基于 BDD 的小型核动力装置安全注射系统可靠性分析[J]. 四川兵工学报,2015(1):52 – 55,77.

[10] 赵新文. 舰艇核动力一回路装置[M]. 北京:海潮出版社,2001.

[11] 陈玲,尚彦龙,蔡琦,等. LOCA 事故下安全注射系统可靠性的 GO-FLOW 法分析[J]. 原子能科学技术,2012(S1):324 – 329.

(责任编辑 唐定国)