文章编号: 1000-6788(2012)09-2087-10 中图分类号: V554 文献标志码: A

基于补偿和不可替代因素合成的人因可靠性分析方法

董学军 [1,2], 陈英武 [1]

(1. 国防科学技术大学 信息系统与管理学院, 长沙 410073; 2. 酒泉卫星发射中心, 酒泉 732750)

摘 要 在安全性要求比较高的环境中, 关键操作失误可能会导致灾难的发生, 因此, 评估关键操作的人因可靠性不仅能为系统灾难评估提供依据, 而且有助于改善关键操作人员的训练水平及工作环境. 本文从因素分解及合成的角度研究人因可靠性, 定义补偿和不可替代因素, 创建补偿和不可替代因素状态合成 (composition of states of irreplaceable and compensation factors, CSICF) 方法. 针对航天器发射工作流程特点, 分析航天器发射人因可靠性因素空间和特性, 构建航天器发射人因可靠性评估模型, 并通过一个模拟实例说明了基于 CSICF 的人因可靠性分析方法的可行性.

关键词 人因可靠性; 工作组可靠性; 补偿和不可替代因素状态合成; 因素空间; 航天器发射

Method of human reliability analysis based on CSICF

DONG Xue-jun[1,2], CHEN Ying-wu[1]

(1. College of Information System and Management, National University of Defense Technology, Changsha 410073, China; 2. Jiuquan Satellite Launch Center, Jiuquan 732750, China)

Abstract In a surrounding expected by the high safety, the critical operation errors could lead to a disaster, therefore, to assess human reliability for critical operator not only provides support for the estimate of the disaster of systems but also is useful to improve the level of training and the condition of the critical operators. In this paper, human reliability is researched by studying the decomposition and composition of factors, compensatory and irreplaceable factors are defined, and the method of composition of states of compensatory and irreplaceable factors (CSICF) is then established. For the characteristic of the basic flow of spacecraft launch engineering, the factors of space and the features of the human reliability of a spacecraft launch are analyzed and the overall human reliability model of spacecraft launch is constructed. Finally, a case analysis demonstrates the application of the human reliability assessment model of a spacecraft launch engineering, which validates the feasibility of the human reliability analysis method of CSICF.

Keywords human reliability; crew reliability; the composition for states of compensatory and irreplaceable factors (CSICF); factors space; spacecraft launch

1 引言

高投入、高风险的特点使灾难评估成为航天器发射工程决策的重点. 从公开的资料看, 航天器发射灾难评估主要集中在航天产品、地面发射系统和测控设备等关键点或重点环节, 对人因可靠度的评价相对比较薄弱. 航天器发射工程实践数据显示, 人因差错曾造成多次任务发射失败、终止或工期严重延误 [1−2], 单纯从产品、设备和环境等实物方面进行灾难评估不仅不能全面、客观地反映航天器发射工程的安全性, 也不能满足航天器发射任务决策和组织流程改进等方面的需求. 因此, 研究航天器发射工程人因可靠性具有重大的现实意义.

人因可靠性是用来描述人的绩效的术语, Dhillon 给出的定义是在规定的最小时间内 (如果有时间要求), 在系统运行的任一阶段, 人员成功完成任务或工作的概率 [3]. 在这一定义下, 人因可靠性分析 (human reliability analysis, HRA) 的目的是如何获取这个概率值, 并趋向于通过假设检验等手段来确定人为差错的概率

收稿日期: 2012-01-19
资助项目: 国家自然科学基金 (70971131, 71071156)
作者简介: 董学军 (1969–), 男, 博士研究生, 高级工程师, 研究方向: 装备采办与项目管理, E-mail: df_dongxuejun@163.com; 陈英武 (1965–), 男, 博士, 教授, 博士生导师, 研究方向: 系统规划与管理决策, E-mail: ywchen@nudt.edu.cn.

分布 - 可靠度 [4], 这与传统的系统 (实物) 可靠性分析手段基本相同. 但是, 传统的系统可靠性分析手段有一个前提, 即系统的失效率不受应用场景的影响, 而人因可靠性很明显无法满足这一前提, 因此, 采用这种手段得到的人因可靠度值得商榷. 1994 年, Kirwan[5] 提出 HRA 的主要目标是正确评估人为差错风险和寻求降低人为差错影响的方式, 因此对人因可靠性的分析可以转向人为差错的分析, 具体过程分为差错辨识、差错频率确定和差错规避措施设计三个阶段. 人为差错的诱因有很多, 其影响机理十分复杂, 没有一种 "理论上完全正确的" 的方法能遍历所有诱因并获取其机理, 但普遍认为除了偶尔出现的随机差错之外, 人为差错的主要诱因有训练水平、任务本质、人机交互界面质量、环境因素和任务执行时间, 有关这五类因素如何影响人的工作效率 (human performance) 的研究已取得很多有益的结果 [6]. 总之, 关于人因可靠性至少有两个方面已经取得共识, 一是人因可靠性水平不是保持不变的, 它受到任务时间和工作环境等因素的影响; 二是不同性质的任务所对应的人因可靠性水平也是不同的.

习惯上将 20 世纪 90 年代以前出现的 HRA 方法统称为第一代 HRA 方法, 常用的有 30 多种 [7], 其中 THERP (technique for human error rate prediction)、HEART (human error assessment and reduction technique)[8]、HCR (human cognitive reliability)[9] 和 OAT (operator action trees)[10] 等方法是它们的代表. 第一代 HRA 方法一般都利用结构化建模和数学计算等方式追求 "精确" 的分析结果, 虽不断得到完善, 如文献 [11] 提出将班组因素引入传统 HRA 方法, 但仍明显存在以下缺陷: 一是认为人可以同其他物理部件等量齐观, 这显然是由于对认识机理的研究不深所致; 二是一般都采用二叉树逻辑来描述人的行为, 对于复杂行为这种描述方法显然是不够的; 三是未考虑组织管理和安全文化等因素对人因可靠性的影响; 四是缺乏数据支持和对分析结果的验证.

从现有资料看, 可以归为第二代 HRA 方法的只有 ATHEANA (a technique for human event analysis)[12−13]、CREAM (cognitive reliability and error analysis method)[7,14] 和 Mermos 等 [15], 而且 Mermos 因没有建立完整的认知模型而不能说是完全意义上的第二代方法. 第二代方法的共同特征是都认为任务所处的环境条件才是人为差错的决定因素, 并建立了认知模型, 在认知模型的基础上进行 HRA. 尽管第二代 HRA 在第一代 HRA 的基础上有所改进, 但仍存在诸多限制: 一是支持 HRA 的数据不足; 二是行为影响因子仍未考虑组织管理因素的影响; 三是缺少实验验证; 四是未能说明人的行为与环境的动态交互特性.

第三代 HRA 是在第一代和第二代 HRA 方法逐步发展和完善的过程中相伴产生的, 它是一类基于仿真的动态的 HRA[16−17], 较具代表性的有认识环境仿真 CES (cognitive environment simulation)[18], 信息、决策和行为响应模型 IDA (information decision and action)[19], 班组情境下的信息、决策和行为响应模型 IDAC (information decision and action crew context)[20] 等. 第三代 HRA 虽试图克服第一代和第二代 HRA 方法的局限性, 尝试建立基于模拟的动态 HRA 方法, 但仍存在以下问题 [21]: 一是不能处理所有行为; 二是缺少组织因素如何影响人因可靠性的基础; 三是缺少对人的认识动态性和人机交互动态性的真实描绘; 四仿真计算和数据的可用性方面存在局限.

概览 HRA 方法可以看出, 大部分 HRA 方法是应核工业概率风险评估 PRA (probabilistic risk assessment) 的需要提出来的, 如果将这些方法及其数据移植到航天发射领域, 将明显存在以下问题: 一是数据存在质疑, 每次航天器发射工程几乎都是独一无二的, 不仅发生的人因差错不具有重复性, 如 1999 年 NASA 发生的单位换算错误导致火星轨道器烧毁 [2], 就连很多操作也几乎不具有重复性, 因此, 现有 HRA 的概率数据很难移植到航天器发射工程中, 而且也很难建立类似的概率数据; 二是组织管理和安全文化的因素在现有的 HRA 方法中几乎没有被考虑, 而这两个因素在具有严格任务流程和高度重视安全文化建设的航天发射工程领域, 对人因可靠性的影响非常突出; 三是航天器发射工程采用项目管理, 源于核工业系统运营管理的 HRA 方法很难移植到航天器发射工程中. 因此, 需要在继承和借鉴现有 HRA 方法的基础上, 结合航天器发射工程领域人因可靠性的特点研发一种新的 HRA 方法和模型.

对于一个很复杂的因素, 如人因可靠性, 确定其状态往往很困难. 但是, 把一个复杂因素分解为若干较简单的因素, 利用这些较简单因素的状态来合成复杂因素的状态是一条既有效又可行的途径 [22]. 同样, 将人因可靠性分解成一组较为简单的、便于考察其状态的因素, 然后, 通过考察每个简单因素的状态来合成人因可靠性的状态也是可行的. 因此, 本文尝试从考察航天器发射人因可靠性的状态空间出发, 研究航天器发射人因可靠性 CSICF 方法, 建立航天器发射人因可靠度评估模型.

2 因素状态合成方法

某些考察对象可以被看作是由不可替代和补偿两类因素构成的, 如考察一组近似圆柱形水箱的容量, 不可替代因素包括水箱的高、底面周长, 补偿因素包括水箱形状与圆柱形的近似程度. 通过获取所有不可替代因素和主要补偿因素的状态值, 然后按照某种规则合成这些状态值, 就可以获得被考察对象状态的近似值.

2.1 不可替代与补偿因素定义

定义 1　因素空间 [22]. 给定论域 (考察对象) M, $F=\{f|f:U\to X(f)\}$ 是 M 上的一组映射, 称集合族 $\{X(f)\}$ 为 M 上的一个因素空间, 如果满足公理:

a) F 上有代数结构, 使得 $F=F(\wedge,\vee,c,1,0)$ 构成一个完整的布尔代数;

b) $X(0)=\{\theta\}$, 0 为零因素, 只有一个空状态 θ;

c) 对任何 $L\subset F$, 若因素族 L 是独立的, 则 $\vee_{(f\in L)}f=\prod_{f\in L}f$, 这里 $\prod_{f\in L}f$ 是因素的直积

F 叫做因素集, $f\in F$ 叫做因素, $X(f)$ 叫做 f 的状态空间, 1 叫做全因素, $X(1)$ 叫做全空间.

定义 2　标准综合函数. X 是考察对象 M 上的一个因素空间, 且其上所有因素的状态值属于 $[0,1]$, 这时有以下形式: $M_m:[0,1]^m\to[0,1],(x_1,x_2,\cdots,x_m)\to M_m(x_1,x_2,\cdots,x_m)$, 称其为标准综合函数.

定义 3　不可替代因素. X 是考察对象 M 上的一个因素空间, 且其上所有因素的状态值属于 $[0,1]$, x_i 为因素 X_i 的状态值, 当 $x_i=0$ 时, 标准综合函数 M_m 恒有: $M_m\left(x_1,x_2,\cdots,x_{(i-1)},0,x_{(i+1)},\cdots,x_m\right)=0$.

设 $\{X_i\}$ 是 X 中具有上述性质的因素全集, 当 $\prod_i x_i=1$ 时, 标准综合函数 M_m 恒有 $M_m(1,1,\cdots,1)=1$, 则称因素 X_i 在考察对象 M 上为不可替代因素.

定义 4　补偿因素. X 是考察对象 M 上的一个因素空间, 且其上所有因素的状态值属于 $[0,1]$, x_i 为因素 X_i 的状态值, 当标准综合函数 M_m 满足对任何 m 维点 $(x_1,x_2,\cdots,x_m)\in[0,1]^m$, 恒有

a) $M_m(1,\cdots,1,\forall x_i,1,\cdots,1)=1$;

b) $M_m(0,\cdots,0,\forall x_i,0,\cdots,0)=0$;

c) $a<b\Rightarrow M_m(x_1,x_2,\cdots,x_{i-1},a,x_{i+1},\cdots,x_m)\le M_m(x_1,x_2,\cdots,x_{i-1},b,x_{i+1},\cdots,x_m)$.

称因素 X_i 在考察对象 M 上为补偿因素.

2.2 不可替代因素状态合成

公理 1　设 X 是考察对象 R 上的一个因素空间, X 中共有 n 个因素, 其中 m 个是不可替代因素, X_i 和 X_j 分别是 X 上的不可替代因素和补偿因素, 状态值分别是 $x_i\in[0,1]$ 和 $x_j\in[0,1]$, 且有 $\sum x_j=0$, 则, 当对 X_i 进行状态合成以得到考察对象 R 的状态值 R_n 时, 有以下各式成立:

a) $R_n:[0,1]^n\to[0,1]$;

b) $\sum_{i=1}^m x_i=0\Rightarrow R_n=0$;

c) $\prod_{i=1}^m x_i=1\Rightarrow R_n=1$;

d) $a<b\Rightarrow R_n(x_1,x_2,\cdots,x_{i-1},a,x_{i+1},\cdots,x_n|\sum x_j=0)\le R_n(x_1,x_2,\cdots,x_{i-1},b,x_{i+1},\cdots,x_n|\sum x_j=0)$.

上式 a) 说明不可替代因素状态合成结果 $R_n\le 1$; 式 b) 说明当任一不可替代因素的状态为零时, 合成结果 $R_n=0$; 式 c) 说明当所有不可替代因素的状态都为最大值 1 时, 合成结果 $R_n=1$; 式 d) 说明除 x_i 外其他不可替代因素的状态保持不变时, 合成结果 R_n 随 x_i 的增加而增加. 根据性质 b) 和 c), 可以将不可替代因素的积 $\prod_{i=1}^m x_i$ 看作一个变量, 令 $f=\prod_{i=1}^m x_i$, 则 f 与 R_n 之间存在某种对应法则, 该法则即为不可替代因素的合成规则.

经验告诉我们, 人因可靠度与其影响因素间存在近似指数关系, 这种关系可以选择多项式拟合, 也可选择指数型函数曲线拟合. 由于使用多项式拟合需要确定的参数比起指数型函数曲线拟合需要的参数要多, 而且航天发射工程人因可靠性的实践数据严重不足, 拟合参数多数情况下不得不依靠专家经验获取, 因此, 在考察人因可靠性时, 选择指数型函数曲线拟合不可替代因素合成规则要优于选择多项式拟合.

定义 5　不可替代因素合成规则. 设 X 是考察对象 R 上的一个因素空间, $\{X_i|1\le i\le m\}$ 是 R 上不可替代因素的全集, X_j 是 R 上的补偿因素, $x_i\in[0,1]$ 和 $x_j\in[0,1]$ 分别是因素 X_i 和 X_j 的状态值, 且 $\sum x_j=0$, 则有

$$R_n\left(x_1,x_2,\cdots,x_i,\cdots,x_n|\sum x_j=0\right)\approx 1-\mathrm{e}^{-\beta\left(\prod_{i=1}^m x_i\right)^\gamma} \tag{1}$$

β 和 γ 为协同因子, R_n 是 R 与点集 $(x_1,\cdots,x_i,\cdots,x_n|\sum x_j=0)$ 相对应的状态值. 不难证明式 (1) 满足公理 1 中 a)、b)、c) 和 d) 的要求.

2.3 补偿因素状态合成

公理 2 设 X 是考察对象 R 上的一个因素空间, X_i 和 X_j 分别是 X 上的不可替代因素和补偿因素, 状态值分别是 $x_i\in[0,1]$ 和 $x_j\in[0,1]$, r_{et} 为 X_j 对 R_n 的补偿值, 令 $f=\prod_{i=1}^m x_i$, 则当对 X_j 进行状态合成以得到补偿量 r_{et} 的值时, 有以下各式成立

a) $0\le r_{et}(f,x_j)\le \mathrm{e}^{(-\beta f^\gamma)}$;

b) $f=0$ 或 $f=1\Rightarrow r_{et}=0$;

c) $a<b\Rightarrow \frac{r_{et}(a,x_j)}{\mathrm{e}^{-\beta a^\gamma}}\le\frac{r_{et}(b,x_j)}{\mathrm{e}^{-\beta b^\gamma}}$;

d) $a<b, f\ne 0$ 或 $1\Rightarrow r_{et}(f,a)\le r_{et}(f,b)$.

上式 a) 保证 X_j 对 R_n 的补偿不会使 $R_n>1$; 式 b) 保证当 $f=0$ 或 $f=1$ 时, X_j 不起作用; 式 c) 保证随 f 的增加, 在保持 X_j 状态不变的情况下, 不可靠度减少的比重 r_{at} 也会增大; 式 d) 保证在 f 不等于 $0,1$ 时, 补偿值 r_{et} 随 X_j 的增加而增加.

定义 6 补偿因素合成规则. 设 X 是考察对象 R 上的一个因素空间, X_i 和 X_j 分别是 X 上的不可替代因素和补偿因素, 状态值分别是 $x_i\in[0,1]$ 和 $x_j\in[0,1]$, r_{et} 为 X_j 对 R_n 的补偿值, 令 $f=\prod_{i=1}^m x_i$, 则有

$$r_{et}\approx x_j f\mathrm{e}^{-\beta f^\gamma} \tag{2}$$

不难证明式 (2) 满足公理 2 中 a)、b)、c) 和 d) 的要求.

定理 1 设 X 是考察对象 R 上的一个因素空间, X_i 和 X_j 分别是 X 上的不可替代因素和补偿因素, 状态值分别是 $x_i\in[0,1]$ 和 $x_j\in[0,1]$, 令 $f=\prod_{i=1}^m x_i$, 则有

$$R_n\approx 1-(1-x_j f)\,\mathrm{e}^{-\beta f^\gamma} \tag{3}$$

β 和 γ 为协同因子, R_n 是 R 与点 (x_i,x_j) 相对应的状态值.

证明 由定义 5 和定义 6 知

$$\begin{aligned}R_n&=R_n(x_1,x_2,\cdots,x_i,\cdots,x_n|\textstyle\sum x_j=0)+r_{et}\approx 1-\mathrm{e}^{-\beta\left(\prod_{i=1}^m x_i\right)^\gamma}+x_j\prod_{i=1}^m x_i\mathrm{e}^{(-\beta\left(\prod_{i=1}^m x_i\right)^\gamma}\\&=1-\mathrm{e}^{-\beta f^\gamma}+x_j f\mathrm{e}^{-\beta f^\gamma}=1-(1-x_j f)\,\mathrm{e}^{-\beta f^\gamma}.\end{aligned}$$

3 工作组可靠度

航天器发射工程的组织过程表现为在统一任务流程下, 相互衔接而又各自相对独立的活动集合. 集合中的每项具体活动都有预先确定的一组人员来执行, 该组人员称为工作组. 工作组成员间不仅需要协同工作才能达成活动的基本目的, 而且还能相互弥补认识和技能不足、检查遗漏、纠正错误, 因此, 考察工作组内单个成员的可靠性是没有意义的, 需要以工作组为最小单元进行人因可靠性的评估. 影响航天器发射工程人因可靠性的因素有很多, 不同专家出于不同目的或从不同角度观察可能会得出不同结论. 本文从不可替代性和补偿性因素的特点出发, 借鉴当前关于人为差错诱因 HEPF (human error producing factor) 的主要研究成果, 构建人因可靠性因素空间.

3.1 工作组可靠性因素空间

从当前人因可靠性的研究成果看, 普遍认为人因可靠性取决于任务对象、环境条件、操作员、设备状态和组织管理 (包括安全文化) 及它们之间的相互作用. 这些因素之间相互影响和制约, 任一因素只有与其它因素一起考虑时才能判断其状态的好坏, 如环境条件的状态只有与操作员的适应程度相比较时才能得到有效量化, 因此, 单独考察任务对象、环境条件、操作员、设备状态和组织管理的状态或对它们的状态进行量化是没有意义的, 把它们当作人因可靠性的因素空间来分析考察人因可靠度也是不合适的. 深入考察航天器发射工程人因可靠性的特点及其形成过程后就会发现, 从考察任务对象、环境条件、操作员、设备状态和组织管理间的关系入手构建航天器发射工程人因可靠性的因素空间会更接近工程实际. 图 1 是工作组可靠度因素空间的示意. 由于本文以工作组为单位考察航天器发射工程人因可靠度, 所以, 在本文中工作组与人因是同一概念.

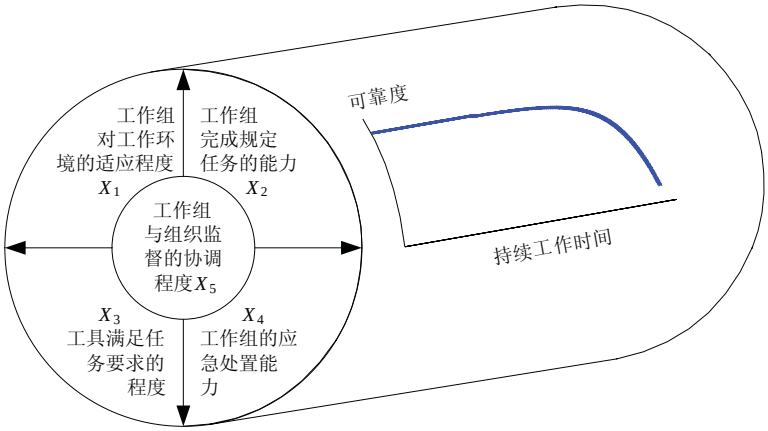

图 1 航天器发射工程工作组可靠性因素空间

工作组对工作环境的适应程度 X_1. 几乎所有的人因可靠性分析方法都认为工作环境是影响工作组绩效输出的重要因素之一, 优越的工作环境能改进工作组的绩效输出, 较差的工作条件会增加工作组出错的概率. 但是, 优越与较差是相对的, 如高度紧张的工作气氛对不同人的影响程度显然是不同的. 事实上, 工作环境对工作组绩效输出的影响程度在于工作组对工作环境的适应程度 X_1. 根据定义 3, X_1 应属于工作组可靠性因素空间中的不可替代因素.

工作组满足任务对能力要求的程度 X_2. THERP 和 HEART 都认为人因可靠度是由任务对象决定的, 并受环境因素的影响, 而且, 它们都针对任务对象给出了基本人因差错概率 NHEP (Nominal Human Error Probability). HCR 和 OAT 认为人因可靠度仅仅取决于可用任务时间, 并给出了获取没有反应或者错误反应概率的方法. 但是, 任务的复杂程度和难易情况以及可用的任务时间都是相对的, 如准确判断运载器飞行状态, 对于经验丰富的人和很少有相关经历的人其复杂和难易程度、以及对时间的要求显然不同. 事实上, 一项有明确要求的任务 (包括可用任务时间) 对工作组可靠度的影响程度取决于工作组完成该任务的能力, 或者说在于工作组完成任务的能力与该任务对工作组能力要求间的匹配程度, 称为工作组满足任务对能力要求的程度 X_2. 根据定义 3, X_2 属于工作组可靠性因素空间中的不可替代因素.

工具满足任务要求的程度 X_3. 显然, 工作组使用的工具对工作组犯错概率有较大影响, 与工作组承担任务相匹配的工具, 不仅能减少工作组犯错的可能性, 而且能在工作中及时发现错误征兆, 便于工作组适时采取预防和纠正措施, 有效避免错误发生或错误后果的扩大. 显然, 工具对工作组犯错概率的影响程度在于工具满足任务要求的程度 X_3, 满足要求的程度越高, 越利于工作组可靠性的提高. 依据定义 3, 其在工作组可靠性因素空间中属于不可替代因素的范畴.

工作组满足应急处理能力要求的程度 X_4. 多数航天器发射工程都带有创新性, 工程实施中的非正常情况难以避免. 对于可以预测到的潜在问题, 人们会针对其类别和影响大小, 事前制定应急处置方案 (预案), 当其发生时, 工作组可按照应急预案的约定开展行动. 对于人们没有预测到的潜在问题, 当其发生时, 除按照约定的组织原则进行处置外, 还需要工作组对正在发生的情景进行快速的判断并开展行动. 显然, 非正常情景发生的概率以及非正常情景发生时工作组的处置能力是影响工作组可靠度的重要因素之一, 因此, 工作组满足应急处理能力要求的程度 X_4 被定义为工作组可靠性因素空间中的第 4 个因素. 依据定义 3, 其属于不可替代因素的范畴.

组织监督的适当程度 X_5. Reason 认为人误是结果不是原因, 人误的产生是由其上游因素 —— 工作环境和组织因素引起的 [23]. Shappell 和 Wiegmann 在分析了数以千计的人因导致飞行事故报告的基础上, 提炼出人的因素分析与分类系统 (the human factors analysis and classification system, HFACS) [24] 框架. 由于在给定任务、规定条件后, 组织因素中与工作组可靠性直接相关的是组织监督, 显然, 合理的有效的组织监督能减少工作组犯错的可能性, 理论上讲, 监督越细致、越严格, 工作组犯错的可能性越小. 但是, 监督受效率的制约, 同时, 监督会影响工作组的心理和生理, 过度的监督不仅不可行, 而且也不一定能达到预期的效果. 所以不能以组织监督的精细和严格程度来考察组织监督的有效性, 代之的是考察组织监督的适当程度 X_5. 工程实际中, X_5 是连接其它因素 X_1、X_2、X_3 和 X_4 的纽带, 根据定义 4, X_5 应属于工作组可靠性中的补偿因素.

除因素 X_1、X_2、X_3、X_4 和 X_5 外, 人员的精神和生理状态、训练水平、人机交互界面、规程和计划的可用性以及应急预案的完整性等明显影响人因可靠性的因素没有纳入航天器发射人因可靠性因素空间, 原因是人员的精神和生理状态可并入 X_1 的考察中, 训练水平可并入 X_2 和 X_4 的考察中, 人机交互界面可并入 X_1 和 X_3 的考察中, 规程和计划的可用性可并入 X_5 的考察中, 这样做不仅简化了工作组可靠性因素空间, 而且可以将因素状态的考察工作与航天器发射工程工作流程中的演练和试验相结合, 避免人力、财力和时间上的浪费.

图 1 中时间 - 可靠度曲线反映了工作组可靠度与工作组连续工作时间的关系. 在长时间的工作过程中, 受环境、任务压力和生理节律等因素的影响, 工作组可靠度随时间持续增长呈下降趋势, 通过分析这种影响机理来确定工作组可靠性曲线, 对于确定合理的工作流程以减少工作组差错是非常有意义的.

3.2 工作组可靠度分析

设因素 X_1, X_2, X_3, X_4, X_5 的状态为闭区间 $[0,1]$ 上的连续值, 工作组可靠度为 R, 依据航天器发射工程特点, R 可以看成有两部分组成, 一部分是工作组完成正常工作的可靠性 R_n, 另一部分是工作组处置潜在问题的可靠性 R_a. 设潜在问题发生的可能性为 p, 则工作组可靠度可表示为 $R=(1-p)R_n+pR_a$.

3.2.1 正常情况下工作组可靠度模型

正常情况是指与被考察工作组相关的各系统工作正常, 工程按预定的任务流程实施. 正常情况下, 因素 X_1, X_2, X_3 是 R_n 上的不可替代因素, 设其状态值分别是 x_1^n, x_2^n, x_3^n, X_5 是 R_n 上的补偿因素, 设其状态值是 x_5^n, 当 $x_5^n=0$ 时, 由式 (1) 得

$$R_n\left(x_1^n, x_2^n, x_3^n, x_5^n | x_5^n=0\right) \approx 1-\mathrm{e}^{-\beta\left(x_1^n x_2^n x_3^n\right)^\gamma} \tag{4}$$

图 2 演示了不可替代因素 X_1, X_2 和 X_3 的状态合成过程及其相互影响的关系, 表现在: a) 因素 X_1, X_2 和 X_3 任一因素的状态值为 0, 则 R_n 为 0, 反映了因素 X_1, X_2 和 X_3 的不可替代性; b) 因素 X_1, X_2 和 X_3 均达到最大值 1 时, R_n 非常接近最大值 1, 反映了因素 X_1, X_2 和 X_3 作为不可替代因素空间的完整性; c) 因素 X_1, X_2 和 X_3 的合成结果与 X_1, X_2 和 X_3 的状态值成伪指数关系, 大小取决于三者状态值的积.

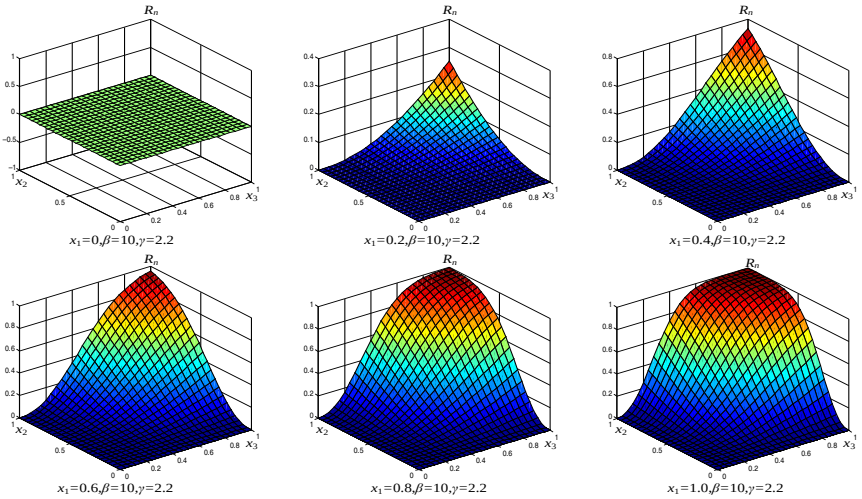

图 2 不可替代因素状态合成效果图

令 $f=x_1^n x_2^n x_3^n$, 协同因子 β 和 γ 对 R_n 的影响见图 3. 从图 3 可以看出, 当 $\beta\in[6,10], \gamma\in[2,6]$ 时, R_n 对 f 的取值较为敏感.

由式 (2) 得

$$r_{et} \approx x_1^n x_2^n x_3^n x_5^n \mathrm{e}^{-\beta\left(x_1^n x_2^n x_3^n\right)^\gamma} = x_5^n f \mathrm{e}^{-\beta f^\gamma} \tag{5}$$

$$r_{at} \approx \frac{r_{et}}{\mathrm{e}^{-\beta f^\gamma}} \approx \frac{x_5^n f \mathrm{e}^{-\beta f^\gamma}}{\mathrm{e}^{-\beta f^\gamma}} = x_5^n f \tag{6}$$

由式 (3) 得

$$R_n \approx 1-\left(1-x_1^n x_2^n x_3^n x_5^n\right)\mathrm{e}^{-\beta\left(x_1^n x_2^n x_3^n\right)^\gamma} = 1-\left(1-x_5^n f\right)\mathrm{e}^{-\beta f^\gamma} \tag{7}$$

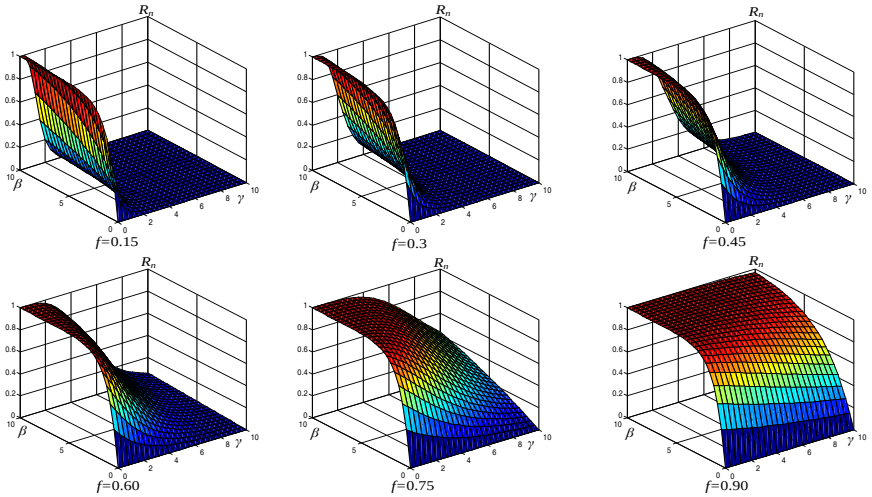

图 3　β 和 γ 对函数 R_n 的影响图

图 4 (a) 反映了式 (5) 中 r_{et} 与 f 和 x_5^n 的关系, 图 4 (b) 反映了式 (6) 中不可靠度下降百分比 r_{at} 与 f 和 x_5^n 的关系, 图 4 (c) 反映了式 (7) 中正常情况下工作组可靠度 R_n 与 f 和 x_5^n 的关系.

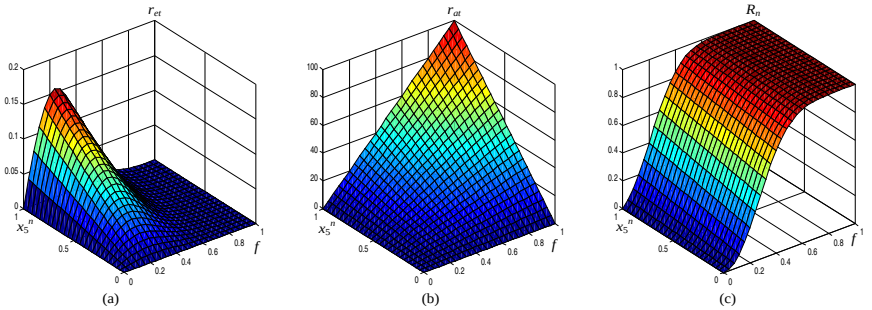

图 4　补偿因素作用效果图 ($\beta = 10, \gamma = 2.2$)

3.2.2　异常情况下工作组可靠度模型

异常情况是指与被考察工作组相关的系统发生异常, 工程不能按预定的任务流程实施. 异常情况下的因素状态合成方法与正常情况下因素状态合成方法相类似, 不同的是使用因素 X_4 的状态替代 X_2 的状态. 令 $x_1^i, x_3^i, x_4^i, x_5^i$ 分别表示当第 i 种异常情况发生时, 因素 X_1, X_3, X_4, X_5 的状态值, 则

$$R_i\left(x_1^i x_3^i x_4^i x_5^i\right) \approx 1 - \left(1 - x_1^i x_3^i x_4^i x_5^i\right) \mathrm{e}^{-\beta_i\left(x_1^i x_3^i x_4^i\right)^{\gamma_i}} \tag{8}$$

式中 β_i 和 γ_i 是在第 i 种异常情况下的协同因子.

3.2.3　工作组可靠度模型

设第 i 种异常情况发生的概率为 p_i, 综合式 (7) 和 (8) 将工作组可靠度模型 $R = (1-p)\,R_n + pR_a$ 修改为

$$R \approx 1 - \left(1 - \sum_{i=1}^{m} p_i\right)\left(1 - x_1^n x_2^n x_3^n x_5^n\right) \mathrm{e}^{-\beta_n\left(x_1^n x_2^n x_3^n\right)^{\gamma_n}} - \sum_{i=1}^{m} p_i\left(1 - x_1^i x_3^i x_4^i x_5^i\right) \mathrm{e}^{-\beta_i\left(x_1^i x_3^i x_4^i\right)^{\gamma_i}} \tag{9}$$

对于首次建造的创新性较强的航天器发射工程, 由于没有充分的可供借鉴的经验和方案, 往往会遗漏某些诱发异常事件的 "条件", 导致在人因可靠性评估中对 $\sum_{i=1}^{m} p_i$ 的估计值低于实际值. 为了使工作组可靠度模型更接近实际, 需要补充一种异常情况, 称其为遗漏的异常情况 O (omit), 设其发生的概率为 p_o. 考虑遗漏的异常情况后, 令 $x_1^o, x_3^o, x_4^o, x_5^o$ 为遗漏情况下因素 X_1, X_3, X_4, X_5 的状态值, 式 (9) 修订为:

$$\begin{aligned} R \approx 1 &- \left(1 - \sum_{i=1}^{m} p_i - p_o\right)\left(1 - x_1^n x_2^n x_3^n x_5^n\right) \mathrm{e}^{-\beta_n\left(x_1^n x_2^n x_3^n\right)^{\gamma_n}} \\ &- \sum_{i=1}^{m} p_i\left(1 - x_1^i x_3^i x_4^i x_5^i\right) \mathrm{e}^{-\beta_i\left(x_1^i x_3^i x_4^i\right)^{\gamma_i}} - p_o\left(1 - x_1^o x_3^o x_4^o x_5^o\right) \mathrm{e}^{-\beta_o\left(x_1^o x_3^o x_4^o\right)^{\gamma_o}} \end{aligned} \tag{10}$$

显然, 概率 p_o 以及在遗漏情况下 X_1, X_3, X_4, X_5 的状态 $x_1^o, x_3^o, x_4^o, x_5^o$ 都是无法测量的, 只能根据潜在问题的暴漏程度, 活动涉及的工程技术成熟度等因素凭经验进行判断.

3.2.4 可靠度分析流程

航天器发射工程人因可靠度分析步骤概括为: 确定任务剖面, 选定模型参数, 明确评估标准, 收集相关信息, 评估因素状态, 集结专家意见, 合成因素状态, 确认评估结果, 提交评估报告. 具体流程见图 5.

4 实例分析

由于若干原因, 本实例的场景和数据都经过了技术处理. X-51 航天器发射工程的飞行控制指令发送是一项非常关键的工作, 要求在适宜的时间发送正确的控制指令, 发送时机错误、指令本身错误、漏发或发送顺序错误都可能造成灾难性的后果. 此项工作有 5 人组成的工作组协同完成, 包括 1 名安全指挥员 (负责收集情景信息, 判断、决策发送什么指令), 2 名相关专家 (搜集、判断运载器和航天器的飞行状态, 为指挥员决策提供技术支持), 1 名指令输入操作员 (负责具体指令的输入操作), 1 名指令输入监督员 (负责核实、发送指令). 运载器加注前, 发射场共组织了 2 次飞控设备对接和 5 次飞控指令演练, 7 次活动工作组的表现数据统计见表 1. 运载器加注前, 10 名专家依据飞控指令对接和演练记录, 参考飞控指令发送工作组训练考评情况和相关评审标准, 针对飞控指令发送工作组可靠性给出的评审意见和评审意见可信度分析记录见表 2.

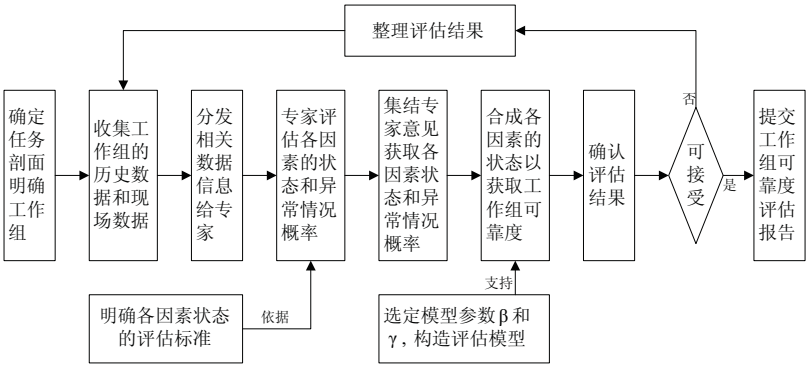

图 5 工作组可靠度分析工作流程

表 1 X-51 航天器发射工程飞控设备对接和演练结果数据统计

	指令输入 正确/累计	指令检查 正确/累计	状态判断 正确/累计	命令下达 正确/累计	指令发送 正确/累计	活动评审 正确/累计	说明
F1	31/32	31/32	0/0	42/42	32/32	2/2	(1) F1 中的指令未
F2	28/28	28/28	0/0	36/36	28/28	1/1	经检查便已发送的
F3	32/32	32/32	16/16	45/45	32/32	2/2	错误计入了指令检
F4	42/42	42/42	16/17	55/56	42/42	1/1	查.
F5	42/42	42/42	17/17	56/56	42/42	1/1	(2) F4 中指令在没
F6	42/42	42/42	17/17	56/56	42/42	1/1	有指挥员命令时便
F7	42/42	42/42	17/17	56/56	42/42	1/1	已发送的错误计入
合计	259/260	259/260	83/84	346/347	260/260	9/9	到命令下达错误.

从表 2 的相似矩阵可以看出, 专家意见之间的一致性非常强, 因此, 可以使用可信度作为权重, 对 x_1, x_2, x_3, x_4, x_5 和 p 的状态值取加权平均, 得: $x_1 = 0.933, x_2 = 0.951, x_3 = 0.986, x_4 = 0.798, x_5 = 0.805$, $p = 0.049$.

考虑到该工程为成熟型任务, 遗漏的异常情况概率 $p_o = 0$, 且 $x_1^n = x_1^i, x_3^n = x_3^i, x_5^n = x_5^i$ 根据专家意见给出的因素状态值与工作组可靠度的关系数据, 采用回归分析的方法获得 $\beta_n = 10, \gamma_n = 2.2, \beta_i = 5, \gamma_i = 2.2$ (所有异常情况下的协同因子值相同), 由式 (7)、式 (8) 和式 (9) 得

正常情况下飞控指令发送工作组可靠度为: 0.9944. 该数据的物理含义是正常情况下工作组发生错发或漏发指令的可能性为 0.0056.

异常情况下飞控指令发送工作组可靠度为: 0.9451. 该数据的物理含义是异常情况下工作组发生错发或

漏发指令的可能性为 0.0549.

飞控指令发送工作组可靠度为: 0.9918. 该数据的物理含义是工作组错发或漏发指令的可能性为 0.082.

5 结论

本文提出 CSICF 方法, 针对航天器发射工程人因可靠性的特点, 建立工作组可靠性因素空间和评估模型. 与其它 HRA 方法相比, 一是 CSICF 方法具有一定的动态性, 它能结合航天器发射工程演练和模拟试验活动, 针对具体人、具体任务和环境采集数据, 进行人因可靠性分析, 避免了第一代和第二代 HRA 方法以静态任务分析作为绩效建模的弊端; 二是 CSICF 方法针对航天器发射工程关键操作的不可重复性, 将现场数据与专家知识相结合, 解决了传统人误数据难以满足新情况的问题; 三是 CSICF 方法考虑了组织因素对人因可靠性的影响, 这是其它 HRA 方法所忽视的. 但是, CSICF 方法中关于协同因子 β 和 γ 的估计问题还有待进一步研究.

表 2　X-51 航天器发射工程飞控指令发送人因可靠度评审专家意见统计表

		专家 1	专家 2	专家 3	专家 4	专家 5	专家 6	专家 7	专家 8	专家 9	专家 10	均值	标准差
	x_1	0.90	0.85	0.95	0.90	0.80	0.85	0.95	0.90	0.80	0.90	0.880	0.0510
	x_2	0.85	0.80	0.90	0.90	0.90	0.80	0.85	0.80	0.85	0.95	0.860	0.0490
	x_3	0.95	0.90	0.90	0.95	1.00	0.85	0.90	0.90	0.95	0.80	0.910	0.0539
	x_4	0.80	0.75	0.75	0.75	0.80	0.85	0.85	0.80	0.75	0.75	0.785	0.0391
	x_5	0.80	0.80	0.75	0.70	0.75	0.65	0.70	0.80	0.75	0.75	0.745	0.0472
	异常概率 p	0.05	0.04	0.03	0.04	0.06	0.08	0.08	0.07	0.05	0.03	0.053	0.0179
	专家 1	1	0.9997	0.9983	0.9981	0.9976	0.9965	0.9975	0.9995	0.9989	0.9953	0.9982	0.0014
	专家 2	0.9997	1	0.9975	0.9968	0.9968	0.9947	0.9959	0.9994	0.9985	0.9946	0.9974	0.0019
	专家 3	0.9983	0.9975	1	0.9990	0.9951	0.9952	0.9976	0.9974	0.9967	0.9982	0.9975	0.0015
	专家 4	0.9981	0.9968	0.9990	1	0.9976	0.9959	0.9974	0.9964	0.9982	0.9962	0.9976	0.0013
相	专家 5	0.9976	0.9968	0.9951	0.9976	1	0.9949	0.9945	0.9956	0.9996	0.9925	0.9964	0.0022
似	专家 6	0.9965	0.9947	0.9952	0.9959	0.9949	1	0.9993	0.9966	0.9949	0.9932	0.9961	0.0020
矩	专家 7	0.9975	0.9959	0.9976	0.9974	0.9945	0.9993	1	0.9977	0.9952	0.9950	0.9970	0.0017
阵	专家 8	0.9995	0.9994	0.9974	0.9964	0.9956	0.9966	0.9977	1	0.9973	0.9945	0.9974	0.0017
	专家 9	0.9989	0.9985	0.9967	0.9982	0.9996	0.9949	0.9952	0.9973	1	0.9938	0.9973	0.0020
	专家 10	0.9953	0.9946	0.9982	0.9962	0.9925	0.9932	0.9950	0.9945	0.9938	1	0.9953	0.0022
	均值	0.9982	0.9974	0.9975	0.9976	0.9964	0.9961	0.9970	0.9974	0.9973	0.9953	1	-
	标准差	0.0014	0.0019	0.0015	0.0013	0.0022	0.0020	0.0017	0.0017	0.0020	0.0022	-	0.0020
	支持度 Sup	9.9816	9.9741	9.9751	9.9755	9.9642	9.9612	9.9702	9.9744	9.9732	9.9533	9.9703	0.0079
	可信度 Crd	0.1001	0.1000	0.1000	0.1001	0.0999	0.0999	0.1000	0.1000	0.1000	0.0999	0.1000	7.9e-05

参考文献

[1] Shayler D J. Disasters and Accidents in Manned Spaceflight[M]. Springer, 2005.

[2] Harland D M, Lorenz R D. Space Systems Failures: Disasters and Rescues of Satellites, Rockets and Space Probes[M]. Springer, 2007.

[3] Dhillon B S. Human Reliability with Human Factors[M]. Oxford, UK: Pergamon Books Inc, 1986.

[4] Liew L. Human reliability evaluation for a keyboarding task[D]. Mississippi State University, 1999.

[5] Kirwan B. A Guide to Practical Human Reliability Assessment[M]. Taylor Francis, 1994.

[6] Staal M A. Stress, cognition and human performance: A literature review and conceptual framework[R]. NASA/TM-2004-212824, 2004.

[7] Hollnagel E. Cognitive Reliability and Error Analysis Method (CREAM)[M]. Oxford: Elsevier Science Ltd, 1998.

[8] Swain A D, Guttmann H E. Handbook of human reliability analysis with emphasis on nuclear power plant applications (NUREG PCR - 1278) [R]. Washington, DC: US Nuclear Regulatory Commission, 1983.

[9] Hanaman G W, Spurgin A J, Lukic Y. Human cognitive reliability model for PRA analysis (NUS 24531) [R]. Draft EPRI Report, Electric Power Research Institute, 1984.

[10] Wreathall J. Operator action trees: An approach to quantifying operator error probability during accident sequences[R]. NUS 24159, San Diego, CA: NUS Corporation, 1982.

[11] 赵军, 童节娟, 刘涛, 等. 核电厂传统人员可靠性分析方法中引入班组因素的研究 [J]. 原子能科学技术, 2011, 45(8): 966–

971.
Zhao J, Tong J J, Liu T, et al. Integrating team factor into current human reliability analysis of nuclear power plant[J]. Atomic Energy Science and Technology, 2011, 45(8): 966–971.
[12] Barriere M. Technical basis and implementation guidelines for a technique for human event analysis (ATHEANA) (NUREG–1624) [R]. Rev.1, Washington, DC: US Nuclear Regulatory Commission, 2000.
[13] Forester J, Bley D, Cooper S, et al. Expert elicitation approach for performing ATHEANA quantification [J]. Reliability Engineering and System Safety, 2004, 83(2): 207–220.
[14] Marseguerra M, Zio E, Librizzi M. Quantitative developments in the cognitive reliability and error analysis method (CREAM) for the assessment of human performance[J]. Annals of Nuclear Energy, 2006, 10(33): 894–910.
[15] Bieder C, Le Bot P, Desmares E, et al. Mermos: EDF's new advanced HRA method[C]// International 4th Conference on Probabilistic Safety Assessment and Management, 1998: 129–134.
[16] Boring R L. Dynamic human reliability analysis: Benefits and challenges of simulating human performance[R/OL]. http://www.inl.gov/technical publications/Documents/3735688.pdf, 2007.
[17] Chang Y H J, Mosleh A. Cognitive modeling and dynamic probabilistic simulation of operating crew response to complex system accidents-Part 1 Overview of the IDAC model[J]. Reliability Engineering and System Safety, 2007, 92(8): 997–1013.
[18] Woods D D, Roth E M, Pople H. Cognitive environment simulation: An artificial intelligence system for human performance assessment, NUREG/CR-4862[R]. Washington DC: USNR, 1987.
[19] Smidts C, Shen S H, Mosleh A. The IDA cognitive model for the analysis of nuclear power plant operator response under accident conditions Part 1 Problem solving and decision making model[J]. Reliability Engineering and System Safety, 1997, 55(1): 51–71.
[20] Chang Y H J, Mosleh A. Cognitive modeling and dynamic probabilistic simulation of operating crew response to complex system accidents Part 5 Dynamic probabilistic simulation of IDAC model[J]. Reliability Engineering and System Safety, 2007, 92(8): 1076–1101.
[21] Zio E. Reliability engineering old problems and new challenges[J]. Reliability Engineering and System Safety, 2009, 94(2): 125–141.
[22] 李洪兴. 因素空间理论与知识表示的数学框架 (I) [J]. 北京师范大学学报: 自然科学版, 1996, 32(4): 470–475.
Li H X. Factor spaces and mathematical frame of knowledge representation (I)[J]. Journal of Beijing Normal University: Natural Science, 1996, 32(4): 470–475.
[23] Reason J. Managing the Risks of Organizational Accidents[M]. Aldershot: Ashgate Pub Ltd, 1997.
[24] Wiegmann D A, Shappell S A. A Human Error Approach to Aviation Accident Analysis[M]. Burlington: Ashgate Publishing Company, 2003.