文章编号:1000-6893(2010)04-0724-08

基于案例知识的系统安全风险模型

冯畅,赵廷弟

(北京航空航天大学 工程系统工程系,北京 100191)

Case Knowledge-based System Safety Risk Model

Feng Chang, Zhao Tingdi

(Department of System Engineering of Engineering Technology, Beijing University of Aeronautics and Astronautics, Beijing 100191, China)

摘 要:对基于案例知识的系统安全风险模型进行了研究。首先,建立了系统安全事件案例知识表达模型。其次,研究了系统知识表达的不确定性问题,以及安全风险决策者的决策类型对度量不确定性的需求;基于现有安全风险模型对不确定性度量能力的欠缺,提出了基于案例知识的系统安全风险概念模型,用损失可能性、损失程度和损失的不确定性来表征系统安全风险。在此基础上,研究了该安全风险模型的建模方法,并举例证明了该模型的有效性。最后,对机长飞行安全风险进行了研究,选取机长年龄、累计飞行小时以及近 90 天飞行小时 3 个指标作为风险因子,应用本文所建基于案例知识的系统安全风险模型,评估了机长飞行安全风险,评估结果合理,可为民航放飞决策提供参考。

关键词:安全;不确定性;风险;风险厌恶;系统;损失;知识表达

中图分类号:V355.1 **文献标识码**:A

Abstract: This article is a study about a knowledge-based complex system safety risk model. First, a knowledge representation model of complex system safety occurrence cases is presented. Second, the uncertainty of knowledge representation as well as the requirement for uncertainty quantifications by the safety risk decision-maker is discussed. Thus, a knowledge-based system safety risk model is presented, where risk is a function of loss probability, loss degree, and loss uncertainty. Then, the modeling method of the proposed model is given, and an instance to demonstrate its application is provided. Finally, the model is used in the safety risk assessment of a civil aircraft flight operation. The attributes of pilot age, total pilot flight hours, and pilot flight hours in the past 90 days are selected as risk factors to assess the flight safety risk of the pilot. The assessment result demonstrates the validity of the proposed model.

Key words: safety; uncertainty; risk; risk-aversion; system; loss; knowledge representation

现有系统使用安全风险评估模型,大多是基于宏观层面,对系统长期的宏观安全水平进行评估。而对于诸如民航飞行活动这样的系统,航空公司/机场等受众希望在某次飞行活动开始前评估其安全风险,从而进行放飞决策。因此,有必要研究微观安全风险模型,以对系统不同状态下其行为的安全风险进行评估与比较,从而为不同系统状态下的系统行为决策提供支持。

概率后果模型[1-3]、损失指数模型[4-6]及危险指数模型[6-10]为宏观安全风险评估领域广泛应用的 3 类典型的安全风险模型。而关于微观安全风险模型的研究尚不多见,已有的如由美国国家航空航天局(NASA)资助、飞行安全基金会(FSF)研究的飞行活动风险评估系统(FORAS)[8-9],以及 FSF 的进近着陆检查单[7]等,均采用危险指数安全风险模型(主要因其对输入数据的要求较低)。

对于系统的微观安全预测而言,尚不能建立"牛顿范式"[11]的解析方程式对其行为进行确定性描述,因此有必要充分利用系统历史行为的案例数据。然而,由于人类认知能力的限制,导致用数据进行知识表达带有不确定性[12-17],并导致系统在相同基本状态下,其行为的安全后果却呈现出随机性。上述 3 类模型中,仅概率后果模型能度量随机性。然而,该模型用严重性等级{1,2,…}的等差级数表征损失程度,考虑安全风险决策者对高严重程度后果具有更强烈的风险厌恶程度,这并不足以很好地描述不同级别安全后果之间损失的量级差距。此外,当系统状态不同而风险可能性及严重程度均相

收稿日期:2009-04-07;**修订日期**:2009-06-29
基金项目:国家"863"计划(2006AA04Z440)
通讯作者:冯畅 E-mail:geniusfc@126.com

同时,概率风险模型将不能对这两种状态的安全风险进行排序。

基于此,本文首先建立了系统安全事件的知识表达模型,以对系统不同状态进行形式化、逻辑化的描述;其次,提出基于该知识表达模型的系统安全风险模型——基于案例知识的系统安全风险模型,用不安全事件发生的可能性、后果严重程度以及后果的波动性 3 个指标来表征系统安全风险;此外,对该安全风险模型的建模方法进行了研究;最后,对民航飞行活动中机长不同状态下的飞行安全风险问题进行了建模分析。

基于案例知识的系统安全风险模型的作用在于:①借鉴概率后果模型,用不安全事件发生概率作为对可能性的度量,实现对系统行为随机性的描述;②考虑安全风险决策者风险厌恶[18]的特点,提出新的损失子模型,用损失级数取代概率后果模型中危险严重性等级,作为对危险严重程度的度量,强调高严重性等级的安全后果对风险的贡献;③考虑安全风险决策者风险厌恶的特点,提出用严重程度方差表征的置信区间作为对安全后果波动性的度量,则可通过波动性对不同系统状态的安全风险进行粒度更细的排序。

1　系统安全事件知识表达模型

1.1　系统安全事件知识表达的理论依据

系统已发生的历史行为统称为安全事件,它既包括安全后果为"正常/安全"的事件(称为正常事件),也包括安全后果为"不安全"的事件(称为不安全事件)。系统安全事件可划分为如图 1 所示 3 个部分:原因、事件链和结果。事件链是系统开始某种行为的过程中发生的非正常事件,它是引发安全后果的显性事件。而以 Heinrich[19]、Bird[20-21]、Surry[22]和 Reason[23-25]等为代表的事故因果论派事故致因理论表明,安全事件的发生是一个长原因链的结果,构成系统的人机环管等多元素的"不安全状态"是系统安全事件链中各元素"显性失效"的隐性原因。即,系统各元素的"危险状态"与系统最终安全后果之间存在着一定的因果联系。因此,安全风险评估的评估者可以在系统开始某种行为之前,依据系统各元素的当前状态,对安全风险进行评估。建立知识表达模型,从而对系统安全事件历史数据中各次案例其初始状态与安全后果之间的映射关系进行逻辑化、形式化的描述,是基于案例的系统安全风险评估的第一步。其中,系统各元素状态所包含的具体属性,可依据系统安全事件历史案例记录、系统安全事件统计分析报告、系统使用安全标准规范等所定义的与安全相关的状态属性而确定。如文献[26]中规定有民航飞行活动的机长、航空器、天气条件等人机环各元素的状态属性。

1.2　系统安全事件的知识表达模型

数据表[12-14]是常用的知识表达基本模型。对于系统安全事件论域而言,一次系统行为案例构成了论域上的一个对象。而系统各元素基本状态属性构成了条件属性集 C,系统行为的安全后果属性构成了结果属性集 D。各次案例记录中各属性的具体取值构成了条件属性值集合 $\boldsymbol{V}_C$ 以及结果属性值集合 $\boldsymbol{V}_D$。取严重性等级 $S=\{1,2,\cdots,k,\cdots,s\}$ 作为结果属性,即 $\boldsymbol{V}_S=\boldsymbol{V}_D$,则系统安全事件的知识表达模型可表示为式(1)所示映射关系,也可如表 1 所示用数据表形象地予以表示。

$$f:\boldsymbol{V}_C\rightarrow\boldsymbol{V}_S \tag{1}$$

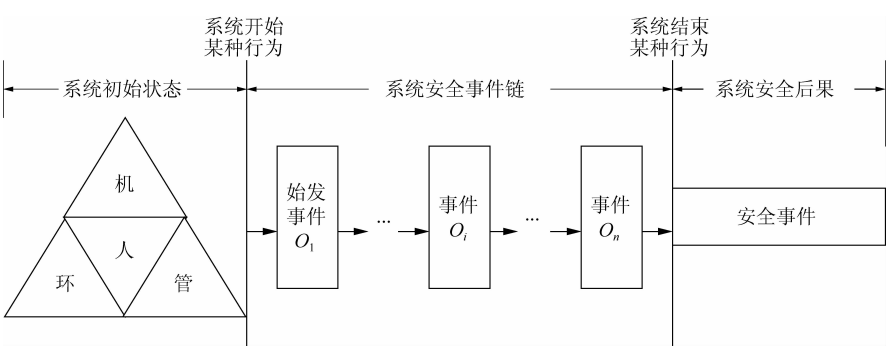

图 1　系统安全事件划分

Fig. 1　Phases of system safety occurrences

表 1 安全事件的知识表达模型

Table 1 Knowledge representation model of safety occurrences

序 号	C				S
	c_1	c_2	…	c_n	
1	v_{c11}	v_{c12}	…	v_{c1n}	s_1
2	v_{c21}	v_{c22}	…	v_{c2n}	s_2
⋮	⋮	⋮		⋮	⋮
i	v_{ci1}	v_{ci2}		v_{cin}	s_i
⋮	⋮	⋮		⋮	⋮
m	v_{cm1}	v_{cm2}	…	v_{cmn}	s_m

设论域上共有 m 个案例对象。则对于其中任意案例对象(设为案例 $j(1\leqslant j\leqslant m)$而言,条件属性值向量 $\boldsymbol{V}_{Cj}=[v_{cj1}\quad v_{cj2}\quad\cdots\quad v_{cjn}]$代表了系统各元素状态的一种可能组合,而结果属性值 $V_{Sj}=s_j$ 则与向量 $\boldsymbol{V}_{Cj}$ 形成了如式(2)所示的映射关系:

$$f_j:\boldsymbol{V}_{Cj}\rightarrow s_j \tag{2}$$

这种映射关系体现了系统各元素初始状态与安全后果之间的联系,是安全风险评估的依据。

2 基于案例知识的系统安全风险概念模型

2.1 知识表达的不确定性

知识理论认为,知识是人们在现有认知水平下,对系统及其行为的描述。知识的作用在于对不同系统及其行为进行分类,通过定义分类族实现对不同系统及其行为的区分。

理论上而言,如果人类的认知能力足够高,则知识粒度(Granulation)[12-14]将足够低,一切系统其行为均可依据"牛顿范式"[11]建立描述其运动的数学方程式,通过求解方程式,实现对系统未来行为的确定性预测。然而这只是理想假设,事实上,人类用以描述系统及其行为的知识是粗粒度的。这种粗粒度导致了人类对系统的知识表达具有不可辨识关系(Indiscernibility)[12-14]、不分明性(Vagueness)[15-16]以及不完备性(Imperfection)[17]等若干不确定性。如:若人类仅能认知"年龄"这一机长条件属性,而不能认知"累计飞行小时",则两次飞行活动中,机长年龄均为 39 岁的两位机长(其累计飞行小时可能分别为 5 000 与 8 000)则会被视为安全条件属性相同,这便构成了论域上的不可辨识关系;而"降水情况"条件属性值{小雨,大雨,雷雨}之间的连续过渡,构成了不分明性;目的地机场的"有无进近雷达覆盖"条件属性值缺失,即造成了案例知识表达的不完备性。

这些不确定性的综合作用,导致了系统知识表达模型中,条件属性值的某种特定组合与结果属性的某种特定组合之间的映射关系,呈现出随机性。即:相同条件属性值组合其结果属性值不同,而不同条件属性值组合其结果属性却相同。人们并不能判断某种条件属性值组合所表征的系统状态到底会导致怎样的安全结果。因此,有必要在安全风险模型中引入对某种安全后果发生随机性的度量。

2.2 安全风险厌恶型决策

对于系统安全论域,安全的重要性决定了如民航飞行签派员等安全工作者其决策类型为安全风险厌恶型(Risk-aversion)[18]。其决策特点为:首先,认为高严重程度后果即意味着高安全风险,即使其发生概率很小;此外,认为相同发生概率与严重程度下,波动性大的系统状态,其可能发生的最严重后果更加严重,该状态安全风险更大。因此,有必要在安全风险模型中引入对损失的严重程度以及波动范围的度量。

2.3 模型表达

综上所述,本文将系统安全风险定义如下。

定义 1 系统安全风险是对系统在某种特定状态下进行某种行为的安全后果损失的度量。它包括 3 个维度:系统在该状态下进行某种行为发生安全损失的可能性、系统在该状态下发生安全损失的程度以及损失的波动性。系统在某状态下进行某种行为的安全风险最终可表示为其发生安全损失的可能性与损失程度的乘积的波动区间。

定义 1 可表示为数学模型

$$R_i=f(P_i,L_i,\theta(L_i))=[P_iL_i-\theta(L_i),P_iL_i+\theta(L_i)] \tag{3}$$

式中:i 代表系统第 i 种可能的状态;损失概率变量 P_i 度量了不安全事件的发生可能性,是对系统安全事件知识表达中条件属性值与结果属性值之间映射关系随机性的描述;损失程度变量 L_i 度量了不安全事件的损失严重程度,损失概率变量与损失程度变量的乘积构成了系统安全风险的基本取值;损失波动性变量 $\theta(L_i)$ 度量了安全风险的波动范围,$\theta(L_i)$ 是置信度 $1-\alpha$ 的函数。因此,安全风险 R_i 最终描述了在一定置信度下,系统在某

状态下其行为不安全的置信区间。

3　基于案例知识的系统安全风险建模

对于系统安全事件知识表达的一般模型而言,条件属性值向量空间中各条件属性值向量 $\boldsymbol{V}_{Cj}$ 代表了系统各元素状态的一种可能组合。设 m 次案例记录中,各案例的条件属性值向量共呈现 $w(1\leqslant w\leqslant m)$ 种不同的状态组合,且其中第 i $(1\leqslant i\leqslant w\leqslant m)$ 种状态组合的案例共 m_i 条,其条件属性值向量计为 $\boldsymbol{V}'_{Ci}$。则条件属性值向量 $\boldsymbol{V}_{Cj}$ 为 $\boldsymbol{V}'_{Ci}$ 的 m_i 条案例,其对应的结果属性值组合不尽相同。设其中后果严重性等级为第 $k(0\leqslant k\leqslant s)$ 级的案例为 m_{ik} 条。则定义如下向量:

(1) 概率向量

定义 $\boldsymbol{P}_i=[p_{i0}\quad p_{i1}\quad\cdots\quad p_{ik}\quad\cdots\quad p_{is}]$ 为 $s+1$ 维概率向量,它表示系统初始状态呈现第 i 种条件属性值组合时,其所有安全后果(含正常与不安全)的概率分布。则分量 $p_{ik}(0\leqslant k\leqslant s)$ 为当系统初始状态呈现第 i 种条件属性值组合时,其结果严重性等级为第 k 级的概率。

定义 $\boldsymbol{P}'_i=[p_{i1}\quad p_{i2}\quad\cdots\quad p_{ik}\quad\cdots\quad p_{is}]$ 为 s 维损失概率向量,它表示系统初始状态呈现第 i 种条件属性值组合时,发生损失(不安全后果)的概率分布。

(2) 后果向量

定义 $\boldsymbol{S}=[0\quad 1\quad\cdots\quad k\quad\cdots\quad s]$ 为 $s+1$ 维后果严重性等级向量,则分量 k 表示了第 k 级严重性等级。

定义 s 维概率向量 $\boldsymbol{S}'=[1\quad 2\quad\cdots\quad k\quad\cdots\quad s]$ 为系统所有不安全后果的严重性等级。

定义 $\boldsymbol{L}_i=[l_{i0}\quad l_{i1}\quad\cdots\quad l_{ik}\quad\cdots\quad l_{is}]$ 为 $s+1$ 维总损失向量,表示系统初始状态呈现第 i 种条件属性值组合时,其所有安全后果的损失分布。分量 $l_{ik}(0\leqslant k\leqslant s)$ 为当系统初始状态呈现第 i 种条件属性值组合时,结果严重性等级为第 k 级的安全事件的损失。易知,$l_{i0}=0$。

定义 s 维损失向量 $\boldsymbol{L}'_i=[l_{i1}\quad l_{i2}\quad\cdots\quad l_{ik}\quad\cdots\quad l_{is}]$ 为系统初始状态呈现第 i 种条件属性值组合时,其不安全后果的损失分布。

则式(3)所定义的系统安全风险模型中,概率变量 P_i、损失变量 L_i 以及波动性变量 $\theta(L_i)$ 的建模方法如下所述。

3.1　损失概率子模型

损失概率子模型度量了系统初始状态呈现第 i 种条件属性值组合时,损失的发生概率,即此时系统所有非正常安全后果的发生概率。

定义系统初始状态呈现第 i 种条件属性值组合时,其损失概率为

$$P_i=\frac{1}{2}\|\boldsymbol{P}'_i\|_1=|p_{i1}|+|p_{i2}|+\cdots+|p_{ik}|+\cdots+|p_{is}| \tag{4}$$

式中:$\|\boldsymbol{P}'_i\|_1$ 为损失概率向量的 1-范数,分量 p_{ik} 的具体求解公式为

$$p_{ik}=\frac{m_{ik}}{m_i} \tag{5}$$

由式(5)易知,当系统初始状态呈现第 i 种条件属性值组合下其严重性等级为第 k 级的安全事件案例记录 m_{ik} 为 0 时,对应的第 k 级安全后果概率 p_{ik} 为 0。

3.2　损失程度子模型

损失程度子模型度量了系统初始状态呈现第 i 种条件属性值组合时,所有非正常安全后果的损失严重程度,可表示为

$$L_i=\boldsymbol{P}''_i\boldsymbol{L}'^{\mathrm{T}}_i \tag{6}$$

式中:$\boldsymbol{P}''_i$ 为折合概率向量,其定义为

$$\boldsymbol{P}''_i=\begin{cases}\boldsymbol{P}'_i/\|\boldsymbol{P}'_i\|_1 & \|\boldsymbol{P}'_i\|_1\neq 0\\ \boldsymbol{0} & \|\boldsymbol{P}'_i\|_1=0\end{cases} \tag{7}$$

通常,$\|\boldsymbol{P}'_i\|_1\neq 0$。当 $\|\boldsymbol{P}'_i\|_1=0$ 时,代表系统处于 i 状态时所有案例均为正常飞行活动,显然此时的损失严重程度为 0。

关于损失向量 $\boldsymbol{L}'_i$ 中,具体损失分量 l_{ik} 的计算公式为

$$l_{ik}=k10^k \tag{8}$$

式中:变量 k 为依据行业标准所确定的安全后果严重程度等级。对于风险厌恶者而言,式(8)中用严重性等级构造的损失乘数,打破了概率后果模型中对损失严重程度的等区间划分,更能体现出高严重程度安全后果的高风险贡献,适应安全风险厌恶型决策需求。

3.3　损失波动性子模型

损失波动性子模型是对损失严重程度波动程度的度量,它可表示为样本方差的函数,即

$$\theta(L_i)=t_{1-\frac{\alpha}{2}}(s)\sqrt{\frac{\sigma^2(L_i)}{s+1}} \tag{9}$$

式中:$1-\alpha$ 为置信度;s 为严重程度等级。

由中心极限定理可知,当样本量 n 足够大时,随机变量 $Y=(\overline{L}-E(L))/\sqrt{D(L)/n}$ 近似服从标

准正态分布。而由于方差 $D(L)$ 未知，实际计算时只能用样本方差 $\sigma^2(L)$ 来代替 $D(L)$，则统计量 $T=(\overline{L}-\mu(L))/\sqrt{\sigma^2(L)/n}$ 服从自由度为 $n-1$ 的 t 分布[27]。

当系统初始状态呈现第 i 种条件属性值组合时，所有案例损失样本均值 $\overline{L_i}$ 及损失样本方差 $\sigma^2(L_i)$ 的求解公式为

$$\overline{L_i}=\sum_{k=0}^{s}p_{ik}l_{ik}=p_{i0}\cdot 0+\sum_{k=1}^{s}p_{ik}l_{ik}=$$
$$[p_{i1}\quad p_{i2}\quad\cdots\quad p_{is}][l_{i1}\quad l_{i2}\quad\cdots\quad l_{is}]^{\mathrm{T}}=$$
$$\boldsymbol{P}'_i\boldsymbol{L}'^{\mathrm{T}}_i=\|\boldsymbol{P}'_i\|_1\boldsymbol{P}''_i\boldsymbol{L}'^{\mathrm{T}}_i=P_iL_i \tag{10}$$

$$\sigma^2(L_i)=\sum_{k=0}^{s}p_{ik}(l_{ik}-\overline{L_i})^2 \tag{11}$$

由式(10)可知，损失样本均值 $\overline{L_i}$ 即为安全风险模型中损失概率与损失后果严重性的乘积。损失样本均值便是概率乘后果的安全风险模型的统计意义。

综上所述，将概率子模型式(4)、损失子模型式(6)以及不确定性子模型式(9)代入式(3)所建安全风险模型，便可求得当系统初始状态呈现第 i 种条件属性值组合时，其置信度为 $1-\alpha$ 时的安全风险。

3.4 模型有效性例证

设某系统历史案例的知识表达模型如表 2 所示。表中：系统的条件属性组合 C 共呈现 4 种不同的初始状态，依次记为 1～4；$m(S)$ 为案例中系统某状态下发生某种安全后果的次数。

表 2 某系统安全事件知识表达模型

Table 2 Knowledge representation model of safety occurrences of a certain system

C	S	$m(S)$	C	S	$m(S)$
1	2	60	3	2	32
1	1	10	3	1	10
1	0	30	3	0	58
2	2	50	4	2	30
2	1	30	4	1	50
2	0	20	4	0	20

概率风险模型(模型 1)与基于案例知识的系统安全风险模型(模型 2)对于系统状态 1 与状态 2 风险评估结果如表 3 所示。显然，模型 2 强调了高严重程度后果对安全风险的贡献，符合安全风险厌恶者的决策需求，且具有更强的排序能力。该结果验证了损失子模型的有效性。

表 3 某系统状态 1 和状态 2 安全风险评估结果

Table 3 Safety risk assessment of States 1-2

状 态	模型 1	模型 2		
	R	PL	$PL-\theta$	$PL+\theta$
1	1.3	121	120.696	121.304
2	1.3	103	102.695	103.305

注：R 为概率风险模型所求得的风险值，它等于不安全事件发生概率与后果的乘积。

基于案例知识的系统安全风险模型对于系统状态 3 与状态 4 的风险评估结果如表 4 所示。显然，波动性变量增强了该模型的风险排序能力。该结果验证了波动性子模型的有效性。

表 4 某系统状态 3 与状态 4 安全风险评估结果

Table 4 Safety risk assessment of States 3-4

状 态	PL	θ	$PL-\theta$	$PL+\theta$
3	65	0.291	64.709	65.291
4	65	0.278	64.722	65.278

4 民用航空器飞行安全风险评估

机长是民航飞行活动的重要元素。来自中国民用航空局(CAAC)[26,28]、美国联邦航空局(FAA)[29]、美国国家运输安全委员会(NTSB)[30]以及加拿大运输安全理事会(CTSB)[31]等的统计数据均表明，近年来，机组的不安全状态及行为，愈发成为飞行事故的主要原因。现有研究成果表明，机长年龄及经验是两个关键因素。关于飞行事故与机长年龄或某项经验等单个指标之间的关系的研究很多，然而，综合考虑多因素的机长状态的安全风险评估还鲜有人做。本文应用所建立的基于案例知识的飞行安全风险模型，对机长飞行安全风险进行了评估，研究并比较了不同机长状态下的飞行安全风险，评估结果可为放飞决策提供参考。

4.1 案例描述

选取机长年龄、累计飞行小时以及近 90 天飞行小时 3 个机长状态典型参数作为条件属性，依据统计数据进行了案例仿真，从而对机长飞行安全风险进行了评估。其中，100 896 186 次案例安全后果的分布来自于 NTSB 数据库 1994—2003 年美国民航运输飞行统计数据[32]，安全后果随机长年龄及累计飞行小时的联合分布来自于文献[29]以及对中国[26]、美国[33]、加拿大[34]民航飞行事故调查报告的统计。在相同年龄及总飞行经验

状态下,安全后果随近 90 天飞行小时的分布主要来自于文献[35]。

条件属性中,机长年龄被划分为 29 岁以下、30～39、40～49、50～59、60～69 这 5 个状态区间,依次用 $c_1=1\sim5$ 标记;累计飞行小时被划分为 0～5 000、5 000～10 000、10 000～15 000、15 000～20 000、20 000～25 000 这 5 个状态区间,依次用 $c_2=1\sim5$ 标记;近 90 天飞行小时被划分为 0～100、100～200、200～300 这 3 个状态区间,依次用 $c_3=1\sim3$ 标记。结果属性严重性等级 $S=\{0,1,2\}$,0、1、2 分别代表正常飞行活动、事故、重大事故[29-33,35]。理论上而言,机长状态有 75 种可能的组合。而事实上,考虑上述 3 个条件属性之间的相关性,最终得到 42 种实际状态组合,其中 8 种状态组合均未发生不安全事件,易知其安全风险为零。表 5 中仅列出飞行安全风险不为零的 34 种状态的具体案例数据。表中:$m(S=k)$为某种机长状态下第 k 级严重性后果发生的次数;m_{total}为某种机长状态下总的飞行活动案例数。

表 5　机长飞行安全风险评估

Table 5　Pilot aviation safety risk assessment

风险排序	C			民航飞行活动案例数据				机长飞行安全风险评估结果					
				$m(S)$			m_{total}	P	L	$\theta(L)$	PL	$PL-\theta$	$PL+\theta$
	c_1	c_2	c_3	$S=2$	$S=1$	$S=0$							
1	4	2	1	2	20	3	25	8.800×10^{-1}	27.27	2.898×10^{-1}	2.400×10^{1}	2.367×10^{1}	2.433×10^{1}
2	5	3	1	1	10	12	23	4.783×10^{-1}	27.27	2.335×10^{-1}	1.304×10^{1}	1.278×10^{1}	1.331×10^{1}
3	4	3	1	1	15	230	246	6.504×10^{-2}	21.88	2.272×10^{-2}	1.423×10^{0}	1.397×10^{0}	1.449×10^{0}
4	4	2	2	0	7	830	837	8.363×10^{-3}	10.00	8.683×10^{-4}	8.363×10^{-2}	8.265×10^{-2}	8.462×10^{-2}
5	5	3	2	0	3	534	537	5.587×10^{-3}	10.00	8.874×10^{-4}	5.587×10^{-2}	5.486×10^{-2}	5.687×10^{-2}
6	5	4	1	1	6	5 566	5 573	1.256×10^{-3}	37.14	9.969×10^{-4}	4.665×10^{-2}	4.552×10^{-2}	4.779×10^{-2}
7	1	1	1	5	61	35 779	35 845	1.841×10^{-3}	24.39	3.492×10^{-4}	4.492×10^{-2}	4.452×10^{-2}	4.531×10^{-2}
8	3	1	1	5	64	37 451	37 520	1.839×10^{-3}	23.77	3.339×10^{-4}	4.371×10^{-2}	4.333×10^{-2}	4.409×10^{-2}
9	5	3	3	0	2	604	606	3.300×10^{-3}	10.00	6.427×10^{-4}	3.300×10^{-2}	3.227×10^{-2}	3.373×10^{-2}
10	4	2	3	0	3	1 598	1 601	1.874×10^{-3}	10.00	2.981×10^{-4}	1.874×10^{-2}	1.840×10^{-2}	1.908×10^{-2}
11	3	2	1	2	6	66 119	66 127	1.210×10^{-4}	57.50	1.184×10^{-4}	6.956×10^{-3}	6.822×10^{-3}	7.091×10^{-3}
12	4	3	2	0	5	8 368	8 373	5.972×10^{-4}	10.00	7.362×10^{-5}	5.972×10^{-3}	5.888×10^{-3}	6.055×10^{-3}
13	4	5	1	1	2	58 088	58 091	5.164×10^{-5}	73.33	9.518×10^{-5}	3.787×10^{-3}	3.679×10^{-3}	3.895×10^{-3}
14	2	1	1	4	52	696 663	696 719	8.038×10^{-5}	23.57	1.609×10^{-5}	1.895×10^{-3}	1.876×10^{-3}	1.913×10^{-3}
15	5	5	1	0	3	17 720	17 723	1.693×10^{-4}	10.00	2.695×10^{-5}	1.693×10^{-3}	1.662×10^{-3}	1.723×10^{-3}
16	4	4	1	1	10	187 879	187 890	5.854×10^{-5}	27.27	2.972×10^{-5}	1.597×10^{-3}	1.563×10^{-3}	1.630×10^{-3}
17	4	3	3	0	2	16 004	16 006	1.250×10^{-4}	10.00	2.436×10^{-5}	1.250×10^{-3}	1.222×10^{-3}	1.277×10^{-3}
18	3	1	2	1	20	362 674	362 695	5.790×10^{-5}	19.05	1.558×10^{-5}	1.103×10^{-3}	1.085×10^{-3}	1.121×10^{-3}
19	1	1	2	0	19	215 054	215 073	8.834×10^{-5}	10.00	5.589×10^{-6}	8.834×10^{-4}	8.771×10^{-4}	8.898×10^{-4}
20	2	2	1	3	30	1 306 466	1 306 499	2.526×10^{-5}	27.27	7.403×10^{-6}	6.889×10^{-4}	6.805×10^{-4}	6.973×10^{-4}
21	3	1	3	1	9	850 447	850 457	1.176×10^{-5}	29.00	6.558×10^{-6}	3.410×10^{-4}	3.335×10^{-4}	3.484×10^{-4}
22	3	3	1	1	2	839 536	839 539	3.573×10^{-5}	73.33	6.586×10^{-6}	2.620×10^{-4}	2.546×10^{-4}	2.695×10^{-4}
23	2	1	2	1	16	1 741 781	1 741 798	9.760×10^{-6}	21.18	3.229×10^{-6}	2.067×10^{-4}	2.030×10^{-4}	2.104×10^{-4}
24	5	4	2	0	2	128 189	128 191	1.560×10^{-5}	10.00	3.042×10^{-6}	1.560×10^{-4}	1.526×10^{-4}	1.595×10^{-4}
25	3	4	1	0	1	93 281	93 282	1.072×10^{-5}	10.00	2.956×10^{-6}	1.072×10^{-4}	1.038×10^{-4}	1.106×10^{-4}
26	3	2	2	0	2	639 223	639 225	3.129×10^{-6}	10.00	6.101×10^{-7}	3.129×10^{-5}	3.059×10^{-5}	3.198×10^{-5}
27	2	2	2	0	10	3 266 236	3 266 246	3.062×10^{-6}	10.00	2.670×10^{-7}	3.062×10^{-5}	3.031×10^{-5}	3.092×10^{-5}
28	5	5	2	0	1	407 636	407 637	2.453×10^{-6}	10.00	6.765×10^{-7}	2.453×10^{-5}	2.376×10^{-5}	2.530×10^{-5}
29	1	1	3	0	10	6 918 155	6 918 165	1.445×10^{-6}	10.00	1.261×10^{-7}	1.445×10^{-5}	1.431×10^{-5}	1.460×10^{-5}
30	2	1	3	0	10	9 173 458	9 173 468	1.090×10^{-6}	10.00	9.506×10^{-8}	1.090×10^{-5}	1.079×10^{-5}	1.101×10^{-5}
31	4	5	2	0	1	1 975 086	1 975 087	5.063×10^{-7}	10.00	1.396×10^{-7}	5.063×10^{-6}	4.904×10^{-6}	5.222×10^{-6}
32	4	4	2	0	3	6 388 260	6 388 263	4.696×10^{-7}	10.00	7.477×10^{-8}	4.696×10^{-6}	4.611×10^{-6}	4.781×10^{-6}
33	2	2	3	0	4	17 202 227	17 202 231	2.325×10^{-7}	10.00	3.206×10^{-8}	2.325×10^{-6}	2.289×10^{-6}	2.362×10^{-6}
34	4	4	3	0	2	12 212 855	12 212 857	1.638×10^{-7}	10.00	3.193×10^{-8}	1.638×10^{-6}	1.601×10^{-6}	1.674×10^{-6}

4.2 案例安全风险评估及结果分析

依据式(3),得到上述 42 种机长状态的安全风险及其排序(95%的置信度)如表 5 所示,其风险分布矩阵如表 6 所示。由评估结果可知:

(1) 安全风险与机长状态之间存在非线性关系,机长飞行安全风险的分布并非随着机长年龄及经验的增加而单调降低。

(2) 对表 6 中 5 个风险分布矩阵进行逐行及逐列比较,易知,飞行安全风险随着机长总飞行经验的增加而降低,同时也随着机长近期飞行经验的增加而降低。即飞行安全风险与机长总飞行经验及近期飞行经验之间存在着较强的线性关系,因此飞行安全风险关于机长状态的非线性分布主要受机长年龄的影响。

(3) 由表 5 可知,30～39 以及 40～49 年龄段的机长其飞行事故次数所占比例最大,然而,该年龄段机长飞行任务也最为频繁。通过表 6 可以看出,总飞行经验小于 5 000 飞行小时的机长,其飞行安全风险排序为 40～49 岁＞29 岁以下＞30～39 岁;总飞行经验 5 000～10 000 飞行小时的机长,其飞行安全风险排序为 50～59 岁＞40～49 岁＞30～39 岁;总飞行经验均为 10 000～15 000 飞行小时,以及 15 000～20 000 飞行小时的机长,其飞行安全风险排序为 60～69 岁以上＞50～59 岁＞40～49 岁。

表 6 飞行安全风险分布矩阵

Table 6 Aviation safety risk distribution matrix

c_2	风险排序														
	$c_1=1$			$c_1=2$			$c_1=3$			$c_1=4$			$c_1=5$		
	$c_3=1$	$c_3=2$	$c_3=3$	$c_3=1$	$c_3=2$	$c_3=3$	$c_3=1$	$c_3=2$	$c_3=3$	$c_3=1$	$c_3=2$	$c_3=3$	$c_3=1$	$c_3=2$	$c_3=3$
1	7	19	29	14	23	30	8	18	21	—	—	—	—	—	—
2	—	—	—	20	27	33	11	26	35	1	4	10	—	—	—
3	—	—	—	—	—	—	22	35	35	3	12	17	2	5	9
4	—	—	—	—	—	—	25	35	35	16	32	34	6	24	35
5	—	—	—	—	—	—	—	—	—	13	31	35	15	28	35

飞行安全风险与机长状态之间的非线性关系与文献[8]和文献[9]的研究一致,证明本文所建模型合理,该风险评估结果对飞行签派具有一定的参考价值。

5 结 论

提出了基于案例知识的系统安全风险模型,用损失的可能性、严重程度以及波动性来度量系统安全风险。该模型能度量安全后果的随机性,并符合安全风险决策者对损失的高严重性以及波动性的厌恶特性。应用该模型进行民用航空器机长飞行安全风险评估,评估结果可为放飞决策提供参考。

参 考 文 献

[1] Kaplan S. On the use of data and judgment in probabilistic risk and safety analysis[J]. Nuclear Engineering and Design, 1986, 93(2): 123-134.

[2] ESA. Risk management, space project management[R]. ESA ECSS-M-00-03B, 2004.

[3] 国防科学技术工业委员会. GJB 900-90 系统安全性通用大纲[S]. 北京: 总装备部军标出版发行部, 1990.
National Defense Science, Technology and Industry Committee. GJB 900-90 General program for system safety [S]. Beijing: Military Standard Publisher of General Ordnance Department, 1990. (in Chinese)

[4] Matthijs K, Andrew E. Transport accident costs and the value of safety[M]. Brussels: European Transport Safety Council, 1997.

[5] Rune E. How much do road accident cost the national economy? [J]. Accident Analysis and Prevention, 2000, 32: 849-851.

[6] 刘铁民, 张兴凯, 刘功智. 安全评价方法应用指南 [M]. 北京: 化学工业出版社, 2005.
Liu Tiemin, Zhang Xingkai, Liu Gongzhi. Safety assessment method application guideline[M]. Beijing: Chemical Industry Press, 2005. (in Chinese)

[7] Flight Safety Foundation. CFIT checklist: evaluate the risk and take action[R]. Flight Safety Foundation, Rev. 2. 3/1, 000/r, 2007.

[8] Hadjimichael M. A fuzzy expert system for aviation risk assessment[J]. Expert System with Applications, 2009, 36(3): 6512-6519.

[9] Hadjimichael M. Flight operations risk assessment system—FORAS applied: first results[C]// 60th International Air Safety Seminar. 2008: 85-90.

[10] Bastos L C M. On-demand part 135 operator risk management model[C]// 60th International Air Safety Seminar. 2008: 91-107.

[11] Newton S. Philosophiae naturalis principia mathematica [M]. London: Joseph Streater, 1687.

[12] Pawlak Z, Skowron A. Rudiments of rough sets[J]. Information Sciences, 2007, 177(1): 3-27.

[13] Pawlak Z, Skowron A. Rough sets: some extensions[J]. Information Sciences, 2007, 177(1): 28-40.

[14] Pawlak Z. Rough set approach to knowledge-based decision support[J]. European Journal of Operational Research, 1997, 99(1): 48-57.

[15] Russell B. Vagueness[J]. Australian Journal of Philosophy, 1923, 1(2): 84-92.

[16] Zadeh L A. Fuzzy sets[J]. Information and Control, 1965, 8(3): 338-353.

[17] Deng J L. Control problems of grey systems[J]. Systems & Control Letters, 1982, 1(5): 288-294.

[18] Charles S T, Konstantin K. Risk-averse order policies with random prices in complete market andretailers' private information[J]. European Journal of Operational Research, 2009, 196(2): 594-599.

[19] Heinrich W H. Industrial accident prevention[M]. New York: McGraw-Hill, 1941.

[20] Bird F E. Management guide to loss control[M]. Atlanta, GA: Institute Press (Division of International Loss Control Institute), 1974.

[21] Bird F E, Loftus R G. Loss control management[M]. Loganville, GA: Institute Press (Division of International Loss Control Institute), 1976.

[22] Surry J. Industrial accident research: a human engineering appraisal[R]. Toronoto, Canada: University of Toronto, 1969.

[23] Reason J. Human error[M]. Cambridge: Cambridge University Press, 1990.

[24] Reason J. Managing the risks of organisational accidents [M]. Aldershot Hants: Ashgate Publishing Ltd, 1997.

[25] Shappell S, Cott A, Douglas A W. The human factors analysis and classification system—HFACS[R]. FAA DOT/FAA/AM-00/7, 2000.

[26] 中国民用航空总局航空安全办公室. MD-AS-2004-01 民用航空不安全事件的处置程序[S]. 北京: 中国民用航空总局航空安全办公室, 2004.
Civil Aviation Administration of China. MD-AS-2004-01 Civil aviation event disposal program[S]. Beijjing: Civil Aviation Administration of China, 2004. (in Chinese)

[27] 张福渊, 郭绍建, 萧亮壮, 等. 概率统计及随机过程[M]. 北京: 北京航空航天大学出版社, 2003.
Zhang Fuyuan, Guo Shaojian, Xiao Liangzhuang, et al. Probability statistic and stochastic process[M]. Beijing: Beijing University of Aeronautics and Astronautics Press, 2003. (in Chinese)

[28] 中国民航航空安全信息系统航空器飞行不安全事件最终报告数据库[DB/OL]. [2009-03-26]. http://218.78.217.36.
Civil aviation safety information system-aircraft flight event final report database[DB/OL]. [2009-03-26]. http://218.78.217.36. (in Chinese)

[29] Dana B, Kurt M J, David J S. Pilot age and accident rates report 3: an analysis of professional air transport pilot accident rates by age[R]. FAA AAM-00-A-HRR-520, 2003.

[30] National Transportation Safety Board. Annual review of aircraft accident data: U.S. air carrier operations calendar year 2004[R]. National Transportation Safety Board NTSB/ARC-08/01 PB2008-108720, 2007.

[31] Transportation Safety Board of Canada. Statistical summary aviation occurrences 2005[R]. National Transportation Safety Board of Canada Cat, TU1-3/2005 ISBN 0662-49087-8, 2006.

[32] NTSB database. Table 5 Accidents, fatalities, and rates, 1988 through 2007, for U. S. air carriers operating under 14 CFR 121, scheduled and nonscheduled service (airlines)[EB/OL]. [2009-03-26]. http://www.ntsb.gov/aviation/Table5.htm.

[33] National transportation safety board[DB/OL]. [2009-03-26]. http://www.ntsb.gov/aviation/aviation.htm.

[34] Transportation safety board of Canada [DB/OL]. [2009-03-26]. http://www.tsb.gc.ca/en/

[35] Grindley G A. Human factors in aviation accidents[R]. UMI 1406779, 2001.

作者简介:

冯畅(1982－)　女,博士。主要研究方向:系统安全工程。

Tel: 010-82317665

E-mail: geniusfc@126.com

(编辑:徐晓)