基于 GSPN 的飞机前轮转弯系统安全性评估

赵 喆 贾玉红 郑 昕 周于添

(北京航空航天大学 航空科学与工程学院, 北京 100191)

摘 要: 为解决在缺乏统计数据时无法对系统安全性进行评估的问题,提出将系统广义随机 Petri 网(GSPN,Generalized Stochastic Petri Nets)与经典评估相结合的方法. 以某型尚处于设计阶段的飞机前轮转弯系统为研究对象,通过分析该系统结构功能图,建立出系统故障类型和影响分析(FMEA,Failure Modes and Effects Analysis)表;依照经典公式,求出系统各单元及其故障类型的故障率、维修度、平均无故障时间和平均维修时间等数据;将求得的数据与前轮转弯系统的 GSPN 模型相结合,利用 TimeNET 软件求得系统各故障类型的稳态失效概率;联立经验公式及危险度矩阵图对系统的安全性进行评估. 经测评,该型飞机前轮转弯系统安全性符合设计要求.

关 键 词: 广义随机 Petri 网; 安全性评估; 前轮转弯系统; 故障类型

中图分类号: V 215.7

文献标识码: A **文 章 编 号**: 1001-5965(2011)12-1546-06

Security evaluation of nose wheel steering systems based on GSPN methods

Zhao Zhe Jia Yuhong Zheng Xin Zhou Yutian

(School of Aeronautic Science and Engineering, Beijing University of Aeronautics and Astronautics, Beijing 100191, China)

Abstract: To solve the problem of how to evaluate the safety of a system without relative statistical data, the generalized stochastic petri nets(GSPN) and classical evaluating method were hung together. Taking a certain type of airplane's nose wheel steering system, which was still at the stage of design, as an example, the failure modes and effects analysis (FMEA) list was set up by analyzing system's function structure figure. The failure rate, maintenance rate, the mean time between failure and the mean time of the maintenance were calculated by the experiential formula. According to these parameters and the nose wheel steering system's GSPN model, the steady failure probabilities were calculated by the TimeNET software package. The safety of the nose wheel steering system was evaluated with the experiential formula and the risk matrix. After the evaluation, this nose wheel steering system conforms to the design demands.

Key words: generalized stochastic petri nets(GSPN); security evaluation; nose wheel steering system; failure mode

前轮转弯系统被用以完成飞机地面方向操纵以及地面运动过程中的减摆,其安全性将直接影响飞机地面运动安全. 前轮转弯系统的安全性应在设计阶段就予以考虑,并应包括在前轮操纵系统设计范围内. 对于一种已有多年运营记录的机型,其前轮转弯系统的安全性可通过故障类型和影响分析(FMEA,Failure Modes and Effects Analysis)以及经验公式等进行定性和定量分析,但是当飞机处于设计阶段而没有系统相关的统计数据时,经典的安全性评估方法无法对系统进行独立

收稿日期: 2010-11-12; **网络出版时间**: 2011-11-14 17:19; **DOI**: CNKI:11-2625/V.20111114.1719.009

网络出版地址: www.cnki.net/kcms/detail/11.2625.V.20111114.1719.009.html

作者简介: 赵 喆(1986 -),男,安徽马鞍山人,硕士生,buaaic@126.com.

的评估.

为解决这一问题,本文首先通过对前轮转弯系统进行故障类型分析,建立系统的 FMEA 表.然后依照系统故障类型以及独立元件的统计数据,建立出系统的广义 Petri(GSPN, Generalized Stochastic Petri Nets)模型,从而得到系统各故障类型的稳态失效概率,进一步可以计算出系统的故障类型频数比.最终依照经验公式对前轮转弯系统安全性的影响因素及其影响程度进行分析,对系统的安全性进行评估[1-5].

1　故障类型分析

以某型尚处于设计阶段的飞机为例,其前轮转弯系统结构功能图如图 1 所示.该型飞机前轮转弯系统采用电传操纵和液压作动的工作模式,并由机械系统、液压系统和电子电气系统 3 个子系统构成,其中每个子系统都有不同的单元及其相应的故障类型.例如电子电气子系统由脚蹬传感器(正驾驶)、WOW、DOWNLOCK 等元件组成,其中脚蹬传感器(正驾驶)又有"传感器无法工作"和"输出错误数据"两种故障类型.照此方法,从系统到元件再到故障类型逐步分析,进而列出系统的 FMEA 表(见表 1).

表 1　部分故障类型和影响分析(FMEA)截表

单元	故障类型	危害等级
脚蹬传感器(正驾驶)(Pf1)	脚蹬传感器无法工作(Pf1-1)	Ⅲ
	脚蹬传感器输出错误(Pf1-2)	Ⅲ
脚蹬传感器(副驾驶)(Pf2)	脚蹬传感器无法工作(Pf2-1)	Ⅲ
	脚蹬传感器输出错误(Pf2-2)	Ⅲ
WOW(Pf3)	WOW 无法接通(Pf3-1)	Ⅲ
	WOW 无法断开(Pf3-2)	Ⅲ
DOWNLOCK(Pf4)	DOWNLOCK 无法接通(Pf4-1)	Ⅲ
	DOWNLOCK 无法断开(Pf4-2)	Ⅲ
…	…	…
CMS(Pf36)	CMS 无法工作(Pf36-1)	Ⅳ
	CMS 输出错误信号(Pf36-2)	Ⅳ
…	…	…

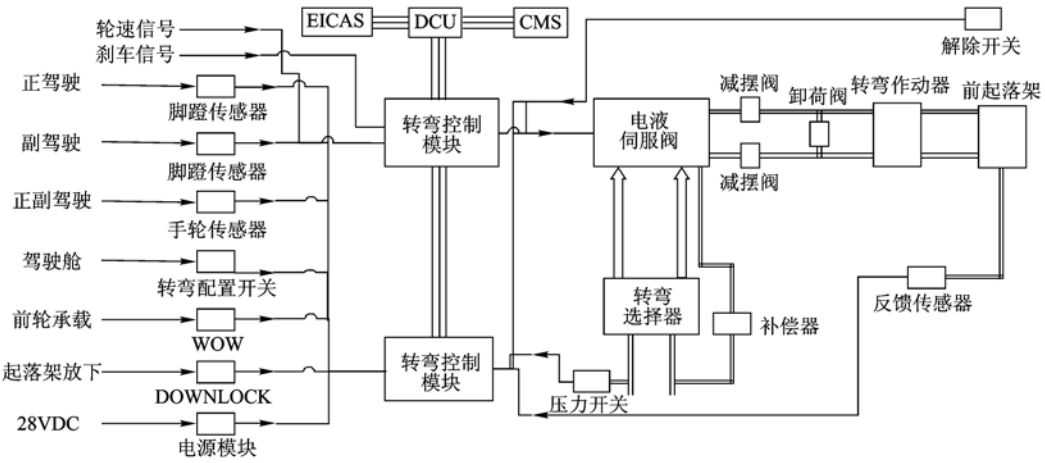

图 1　系统功能结构图

由以上分析可知每个元件在系统中的故障类型,这为后面系统广义随机 Petri 网模型的建立提供了依据.

2　系统建立 GSPN 模型可行性分析

在航空产品中,电子电气系统及液压系统元件的失效事件和维修事件以及机械系统元件的维修事件大都服从指数分布;而机械元件的失效率虽一般呈浴盆曲线分布,但是在忽略机械元件的磨合期和老化期,仅考虑元件在平稳工作期的工作状态(即失效率曲线只取浴盆曲线中间平直段)时,机械元件的失效事件也可视为服从指数分布.所以可以认为,前轮转弯系统所有元件的故障类型的失效事件和维修事件均服从指数分布.由马尔科夫过程理论可知,该型飞机前轮转弯系统故障类型的 GSPN 模型与一个时间参数连续马尔科夫链同构.同时,系统中各元件及其故障类型的失效度和维修度均大于 0(即各状态转移概率均大于 0),且故障类型的状态个数有限(即状态转移矩阵中的元素个数有限),所以根据马尔科夫过程理论可以判定,故障类型的 GSPN 模型可遍历,所以故障类型存在稳态失效概率[6-9].

综上所述,前轮转弯系统可以通过建立广义随机 Petri 网模型求得其各个故障类型的稳态失效概率.

3　系统广义随机 Petri 网的建立

在建立系统的 GSPN 模型时,需要知道元件在各个故障类型下的平均无故障时间 θ_i 和平均维修时间 ω_i,这些参数可由以下方法求得.

假设根据元件独立的统计数据,该元件在某时间内的失效概率为 P_1;从 0 时刻到 t_2 时刻 t_2 个

小时维修时间内的修复概率为 P_2. 则 t_1 时刻元件在该故障类型的失效概率为

$$P_1(t_1) = F_1(t_1) = \begin{cases} 1 - e^{-\lambda_1 t_1} & t_1 > 0 \\ 0 & t_1 \leqslant 0 \end{cases} \quad (1)$$

则元件在该故障类型的失效率为

$$\lambda_1 = -\frac{\ln[1 - P_1(t_1)]}{t_1} \quad (2)$$

元件在该故障类型下的平均无故障时间为

$$\theta_1 = \frac{1}{\lambda_1} = -\frac{t_1}{\ln[1 - P_1(t_1)]} \quad (3)$$

t_2 时刻元件在该故障类型的修复概率为

$$P_2(t_2) = R_1(t_2) = \begin{cases} 1 - e^{-\mu_1 t_2} & t_2 > 0 \\ 0 & t_2 \leqslant 0 \end{cases} \quad (4)$$

则元件在该故障类型的维修度为

$$\mu_1 = -\frac{\ln[1 - P_2(t_2)]}{t_2} \quad (5)$$

元件在该故障类型的平均维修时间[10]为

$$\omega_1 = \frac{1}{\mu_1} = -\frac{t_2}{\ln[1 - P_2(t_2)]} \quad (6)$$

由此可以分别得出系统各元件在不同故障类型下的失效率、维修度、平均无故障时间以及平均维修时间[10](见表 2).

表 2 系统各元件在不同故障类型下的失效率、维修度、平均无故障时间以及平均维修时间

单元	故障类型	失效率 λ/h^{-1}	平均无故障时间/h	维修率 μ/h^{-1}	平均维修时间/h
脚蹬传感器(正驾驶)(Pf1)	脚蹬传感器无法工作(Pf1-1)	2.12×10^{-8}	4.72×10^{7}	0.33	1.96
	脚蹬传感器输出错误(Pf1-2)	2.41×10^{-9}	4.15×10^{8}	0.33	1.96
脚蹬传感器(副驾驶)(Pf2)	脚蹬传感器无法工作(Pf2-1)	2.12×10^{-8}	4.72×10^{7}	0.33	1.96
	脚蹬传感器输出错误(Pf2-2)	2.41×10^{-9}	4.15×10^{8}	0.33	1.96
WOW (Pf3)	WOW 无法接通(Pf3-1)	4.79×10^{-8}	2.09×10^{7}	0.25	4.00
	WOW 无法断开(Pf3-2)	3.16×10^{-8}	3.16×10^{7}	0.25	4.00
DOWNLOCK (Pf4)	DOWNLOCK 无法接通(Pf4-1)	5.27×10^{-8}	1.90×10^{7}	0.24	4.17
	DOWNLOCK 无法断开(Pf4-2)	3.24×10^{-8}	3.09×10^{7}	0.24	4.17
…	…	…	…	…	…
CMS (Pf36)	CMS 无法工作(Pf36-1)	2.55×10^{-10}	3.92×10^{9}	0.19	5.26
	CMS 输出错误信号(Pf36-2)	2.68×10^{-11}	3.73×10^{10}	0.19	5.26
…	…	…	…	…	…

利用 TimeNET 软件依次对系统中不同元件及其故障类型进行建模,并将系统各元件故障类型的平均无故障时间以及平均维修时间带入到模型中. 以脚蹬传感器(正驾驶)为例,该元件有“脚蹬传感器无法工作”以及“脚蹬传感器输出错误”两种故障类型,只要有任意一种故障类型触发,元件便失效;当所有故障类型的触发状态均被解除时,元件便恢复正常. 故该元件由两种故障类型串联而成,如图 2 所示.

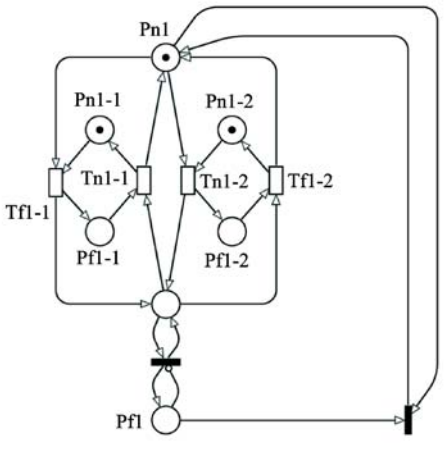

图 2 脚蹬传感器(正驾驶) Petri 网模型

Pn1 表示脚蹬传感器(正驾驶)处于“正常”状态;

Pf1 表示脚蹬传感器(正驾驶)处于“失效”状态;

Pn1-1 和 Pn1-2 分别表示子元件在“脚蹬传感器无法工作”及“脚蹬传感器输出错误”故障类型下处于“正常”状态;Pf1-1 和 Pf1-2 分别表示子元件在“脚蹬传感器无法工作”及“脚蹬传感器输出错误”故障类型下处于“失效”状态;

Tf1-1 和 Tf1-2 分别表示子元件在“脚蹬传感器无法工作”故障类型下从“正常”到“失效”状态的延时时间(即平均无故障时间 θ_1)以及在“脚蹬传感器输出错误”故障类型下从“正常”到“失效”状态的延时时间(即平均无故障时间 θ_2);

Tn1-1 和 Tn1-2 分别表示子元件在“脚蹬传感器无法工作”故障类型下从“失效”到“正常”状态的转移延时时间(即平均维修时间 ω_1)以及子元件在“脚蹬传感器输出错误”故障类型下从“失效”到“正常”状态的转移延时时间(即平均维修时间 ω_2).

在前轮转弯系统里部分元件采取多余度设

计,这些元件由多个子元件组成. 只有当失效的子元件数达到或超过临界值时,元件才会失效;当失效子元件解除失效状态,且失效子元件数小于临界值时,元件便又恢复到正常状态. 例如系统中脚蹬传感器由正副驾驶的脚蹬传感器并联而成,它们的广义随机 Petri 模型如图 3 所示.

Pmn1 表示多余度设计元件脚蹬传感器处于“正常”状态;

Pmf1 表示多余度设计元件脚蹬传感器处于“失效”状态;

Pn1 和 Pn2 分别表示脚蹬传感器(正驾驶)和脚蹬传感器(副驾驶)处于“正常”状态;

Pf1 和 Pf2 分别表示脚蹬传感器(正驾驶)和脚蹬传感器(副驾驶)处于“失效”状态.

将采取多余度设计且具有同一功能的所有的子元件视为一个多余度设计元件(Pmn$i$),与其他单余度设计元件(Pi)一起串联构成系统. 在系统中,只要有一个元件失效,系统便失效;当所有元件正常时,系统才处于正常状态. 系统 Petri 模型如图 4 所示. 依次求得系统中各单余度设计元件和多余度设计元件及其子元件的稳态失效概率,然后再依次求得(子)元件各故障类型的稳态率.

Psn 表示前轮转弯系统处于“正常”状态;

Psf 表示前轮转弯系统处于“失效”状态;

Pmn1 表示多余度设计元件脚蹬传感器处于“正常”状态;

Pmf1 表示多余度设计元件脚蹬传感器处于“失效”状态;

Pn3 和 Pn4 分别表示 WOW 和 DOWNLOCK 处于“正常”状态.

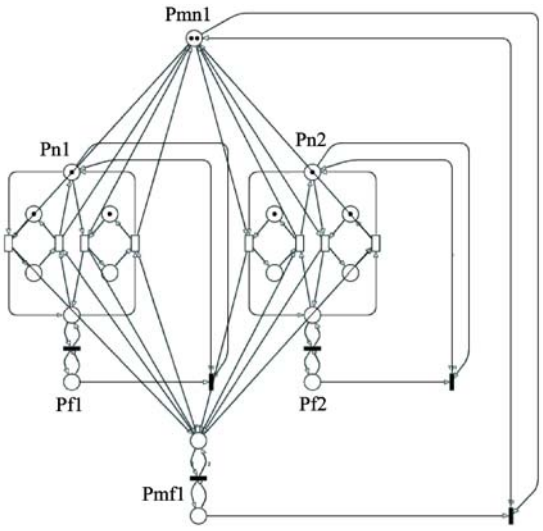

图 3　脚蹬传感器(并联)Petri 网模型

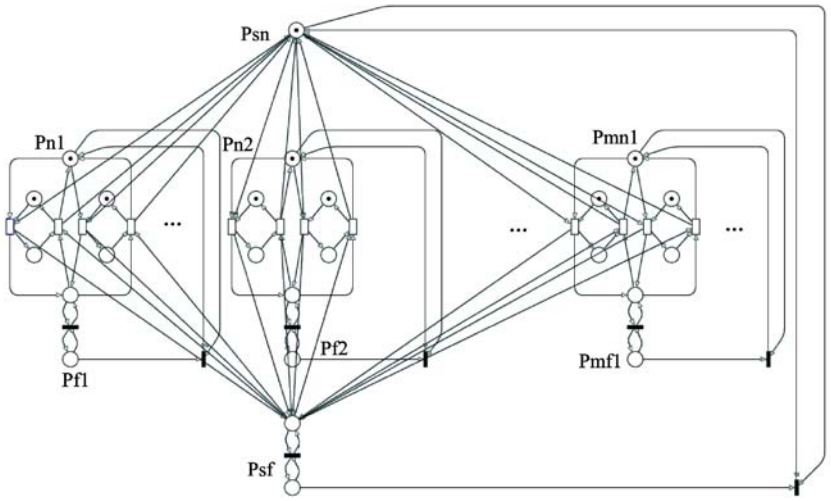

图 4　系统 Petri 模型

4　系统安全性评估

4.1　评估方法介绍

因为系统是离散型系统且存在稳态失效概率,故对于某元件 i 在任意故障模式 i-j 下,由“正常”状态到“失效”状态的稳态失效概率为

$$\tau_{i\text{-}j} = \lim_{n\to\infty} T_{i\text{-}j(N\to F)}(n) = \tau_{i\text{-}j(F)} \tag{7}$$

是方程

$$\tau_{i\text{-}j(F)} = \sum \tau_{i\text{-}j(N)} T_{i\text{-}j(N\to F)} \tag{8}$$

在满足 $\begin{cases}\tau_{i\text{-}j(F)} > 0 \\ \tau_{i\text{-}j(F)} + \tau_{i\text{-}j(N)} = 1\end{cases}$ 条件下的唯一解.

元件 i 由“正常”状态到“失效”状态,稳态失效概率为

$$\pi_i = \lim_{n\to\infty} T_{i(N\to F)}(n) = \pi_{i(F)} \tag{9}$$

是方程

$$\pi_{i(F)} = \sum \tau_{i(N)} T_{i(N\to F)} \tag{10}$$

在满足 $\begin{cases}\tau_{i(F)} > 0 \\ \tau_{i(F)} + \tau_{i(N)} = 1\end{cases}$ 条件下的唯一解.

以上 $T_{i(N\to F)}(n)$ 是转移矩阵 $\boldsymbol{T}_i^n$ 的元素[6].

在系统中,元件的任一故障类型危险度指数由下式计算:

$$C_{\mathrm{m}} = \alpha\beta k_1 k_2 \lambda_{\mathrm{b}} t \tag{11}$$

其中,C_{m} 表示故障类型的危险度指数;α 表示故障类型比;β 表示故障影响概率;k_1 表示运行强度修正系数;k_2 表示运行时及环境条件的修正系数;λ_{b} 表示单元的基本失效率;t 表示完成一次任务所需的运行时间或周期.

单元或系统(有多种故障类型)对应特定故障严重度的危险度指数可由下式计算得出:

$$C_{\mathrm{r}} = \sum_{i=1}^{n} (\alpha\beta k_1 k_2 \lambda_{\mathrm{b}} t)_i \tag{12}$$

其中,C_{r} 表示单元或系统危险度指数;i 表示单元或系统属于特定故障严重度级别的故障类型编号;n 表示单元或系统属于特定故障严重度级别的故障类型总数.

由于实验环境与工作环境相同,故 k_1 和 k_2 取值为 1. α 可按以下方法计算求出:

1) 在采用多余度设计的元件中,失效子零件数达到或超过临界值时元件才会失效;而子元件中只要有一个故障类型触发,该子元件便失效,所以元件的故障类型在整个系统中的故障类型比为

$$\alpha_{ij} = \frac{\tau_{i\text{-}j}(\pi_{pm}/\pi_i)}{\pi_{\mathrm{s}}} \quad 1 \leqslant i \leqslant n, 1 \leqslant j \leqslant k \tag{13}$$

其中,π_{pm} 表示第 m 个多余度设计元件稳态失效概率;π_i 表示第 i 个子元件的稳态失效概率;$\tau_{i\text{-}j}$ 表示第 i 个子元件中第 j 个故障类型的稳态概率;π_{s} 表示系统的稳态失效概率;n 表示系统故障类型个数;k 表示第 i 个元件故障类型个数.

2) 串联在系统中的其他单余度元件,它们的失效由其对应的各个相互独立的故障类型以串联的形式引发(即相互独立的故障类型,只要有一个触发就会导致元件失效),则故障类型在整个电子电气系统中的故障类型比为

$$\alpha_{ij} = \frac{\tau_{i\text{-}j}}{\sum_{i=1}^{n} \pi_i} \quad 1 \leqslant i \leqslant n, 1 \leqslant j \leqslant k \tag{14}$$

其中,n 表示系统元件个数;k 表示第 i 个元件故障类型个数.

β 值计算方法见表 3.

表 3 β 值计算方法

故障影响	发生概率 β
肯定造成损失	$\beta=1$
很可能造成损失	$0.1\leqslant\beta\leqslant1$
可能造成损失	$0\leqslant\beta\leqslant0.1$
没有影响	$\beta=0$

按以上方法将求出的各个参数、故障类型的危险度指数(C_{m})以及系统对应特定故障严重度的危险度指数(C_{r})带入危害性分析表,见表 4.

以故障严重度为横坐标,系统对应特定故障严重度的危险度指数(C_{r})为纵坐标,绘制危险度矩阵图. 按照设计要求,危害等级为Ⅲ的故障类型危险度指数应小于 1×10^{-7},危害等级为Ⅳ的故障类型危险度指数应小于 1×10^{-9},在危险度矩阵图中标出这些安全临界点,并将安全临界点拟合成安全临界线[1],如图 5、图 6 所示.

表 4 危害性分析表

单元		故障类型	失效率 λ/h^{-1}	危害度	α	β	工作时间/h	C_{m}	C_{r}
电子电气设备	脚蹬传感器(正驾驶)(Pf1-1)	脚蹬传感器无法工作(Pf1-1)	2.12×10^{-8}	Ⅲ	3.16×10^{-2}	0.2	3	4.02×10^{-10}	危害等级为Ⅲ的危险度指数 $C_{\mathrm{r}}=3.6\times10^{-8}$;危害等级为Ⅳ的危险度指数 $C_{\mathrm{r}}=4.1\times10^{-10}$
		脚蹬传感器输出错误数据(Pf1-2)	2.41×10^{-9}	Ⅲ	3.60×10^{-3}	0.2	3	5.21×10^{-12}	
	脚蹬传感器(副驾驶)(Pf1-2)	脚蹬传感器无法工作(Pf2-1)	2.12×10^{-8}	Ⅲ	3.16×10^{-2}	0.2	3	4.02×10^{-10}	
		脚蹬传感器输出错误数据(Pf2-2)	2.41×10^{-9}	Ⅲ	3.60×10^{-3}	0.2	3	5.21×10^{-12}	
	WOW(Pf3)	WOW 无法接通(Pf3-1)	4.79×10^{-8}	Ⅲ	7.15×10^{-2}	0.6	3	6.16×10^{-9}	
		WOW 无法断开(Pf3-2)	3.16×10^{-8}	Ⅲ	4.72×10^{-2}	0.6	3	2.68×10^{-9}	
	DOWNLOCK(Pf4)	DOWNLOCK 无法接通(Pf4-1)	5.27×10^{-8}	Ⅲ	7.87×10^{-3}	0.6	3	7.47×10^{-9}	
		DOWNLOCK 无法断开(Pf4-2)	3.24×10^{-8}	Ⅲ	4.72×10^{-2}	0.6	3	2.75×10^{-9}	
	…	…	…	…	…	…	…	…	
	CMS(Pf36)	CMS 无法工作(Pf36-1)	2.55×10^{-10}	Ⅳ	3.81×10^{-4}	0.8	3	2.33×10^{-13}	
		CMS 输出错误数据(Pf36-2)	2.68×10^{-11}	Ⅳ	4.00×10^{-5}	0.8	3	2.57×10^{-15}	
…	…	…	…	…	…	…	…	…	

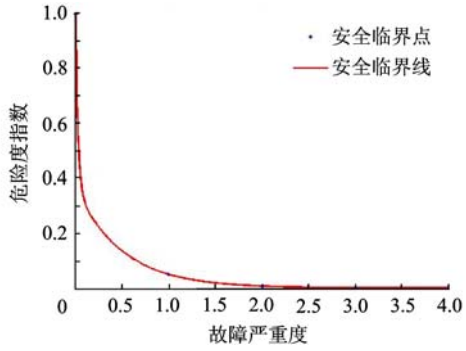

图 5　危险度矩阵图

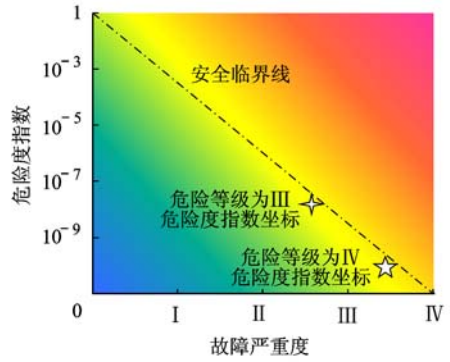

图 6　危险度矩阵图

4.2 数据分析

1）危害等级为Ⅲ的故障类型危险度指数 $C_r = 3.6 \times 10^{-8}$,危害等级为Ⅳ的故障类型危险度指数 $C_r = 4.1 \times 10^{10}$,所处的坐标均在安全临界线以内;

2）系统不同危险等级的故障类型在危险度矩阵图中所对应的坐标距离安全临界线距离都较近.

随着故障严重度和危险度指数的不断增加,故障模式的风险水平也会不断增加.

5　结　论

1）危害等级为Ⅲ的故障类型危险度指数和危害等级为Ⅳ的故障类型危险度指数均小于安全标准规定的临界值,故系统安全;

2）系统的冗余度不是很高,在满足安全性的前提下系统设计较为合理;

3）若想进一步提高系统的安全性,可适当提高危险度较大且危险度指数较高的元件的余度.

参考文献（References）

[1] 王永华,李本威,孙涛. FMECA 在某发动机涡轮部件上的应用[J]. 航空工程与维修 2002(4):27 – 28
Wang Yonghua, Li Benwei, Sun Tao. Application of FMECA on engine turbine parts[J]. Aviation Engineering & Maintenance, 2002(4):27 – 28(in Chinese)

[2] 葛志浩,徐浩军,胡飞. 某型飞机横向操纵系统的飞行安全评估及改进措施[J]. 飞行力学,2005,23(2):39 – 42
Ge Zhihao, Xu Haojun, Hu Fei. Flying security evaluation and improving measures of a certain plane lateral – directional control system [J]. Flight Dynamics, 2005, 23(2): 39 – 42(in Chinese)

[3] 曾德容. 地铁供电系统可靠性和安全性分析方法研究[D]. 西南交通大学电气工程学院:2008
Zeng Derong. Research on reliability and safety evaluation method of metro power supply system [D]. School of Electrical Engineering, Southwest Jiaotong University, 2008(in Chinese)

[4] 刘涛,蔡增杰. 基于 FMECA 和模糊综合评判的飞机起动电磁阀安全性评估[J]. 机械,2009(12):65 – 68
Liu Tao, Cai Zengjie. Accessory safety assessment of airplane start-up electromagnetic valve based on FMECA and fuzzy comprehensive evaluation methods[J]. Machinery, 2009(12):65 – 68(in Chinese)

[5] Von Mayrhauser A, Dube D. Simple and fast approximations for generalized stochastic petri nets[J]. J Systems Software, 1993, 21(2):63 – 177

[6] 汪一亭,魏臻. 基于 Markov 模型的离散事件系统稳态与暂态的分析[J]. 计算机工程与应用,2009,45(3):226 – 228
Wang Yiting, Wei Zhen. Research on steady states and transient states of discrete event system based on markov modle [J]. Computer Engineering and Application, 2009, 45(3):226 – 228(in Chinese)

[7] Chen M F. From Markov chains to non-equilibrium particle systems[M]. Singapore: World Scientific Publishing Co Pte Ltd, 1992

[8] Anderson W J. Continuous-time Markov chains[M]. Berlin: Springer, 1991

[9] Meyn S P, Tweedie R L. Markov chains and stochastic stability [M]. Berlin: Springer, 1993

[10] 陈永,胡晓辉. 基于 GSM-R 铁路无线通信系统的越区切换分析研究[J]. 计算机工程与设计,2009,30(18):4342 – 4345
Chen Yong, Hu Xiaohui. Analysis of handover based on GSM-R wireless railway communications system[J]. Computer Engineering and Design, 2009, 30(18):4342 – 4345(in Chinese)

(编　辑:李　晶)