doi:10.11887/j.cn.201406021 http://journal.nudt.edu.cn

复杂系统故障安全风险评价方法*

蒋 平[1],邢云燕[2],王 冬[1],龚时雨[1]
(1.国防科技大学 信息系统与管理学院,湖南 长沙 410073;
2.国防科技大学 军事高科技培训学院,湖南 长沙 410073)

摘 要:复杂系统的安全风险涉及面广、影响因素多,因此需要系统的、可操作的方法来指导安全风险的评价过程。在系统的各类安全风险中,故障安全风险是由各种故障导致系统发生事故的风险,是最常见的系统安全问题,因此针对复杂系统的故障安全风险评价开展研究。复杂系统故障安全风险评价需要明确的评价参数和评价方法的支持,为此提出了复杂系统故障安全风险评价的流程、分层次的评价参数体系及评价方法,并通过示例来具体说明故障安全风险的评价过程,为解决复杂系统的故障安全风险评价问题提出了可行的思路。

关键词:系统;故障;安全风险;评价参数体系;评价方法
中图分类号:TE48 **文献标志码**:A **文章编号**:1001-2486(2014)06-117-06

Failure safety risk evaluation approach for complex systems

JIANG Ping[1], *XING Yunyan*[2], *WANG Dong*[1], *GONG Shiyu*[1]
(1. College of Information System and Management, National University of Defense Technology, Changsha 410073, China;
2. College of Continuing Education, National University of Defense Technology, Changsha 410073, China)

Abstract: As various issues and impacting factors involved in the safety risk of complex systems, systematic and operational approach was desirable to instruct the evaluation process of safety risk for complex systems. Among the safety risks of a system, failure safety risk, the risk of accidents caused by various failures, is the most common system safety problem, so the evaluation of failure safety risk for complex systems was studied. The evaluation requires the support of explicit parameters and proper approach. Therefore, the paper presented the evaluation process of failure safety risk for complex systems, hierarchical evaluation parameters and approach, and examples were applied to demonstrate the evaluation process in detail. Results show that the proposed evaluation approach provides a feasible solution to evaluate the failure safety risk of complex system.

Key words: system; failure; safety risk; evaluation parameters; evaluation approach

安全性评价也称危险性评价,或称安全评价、危险评价,它是安全性工程的一项主要内容[1]。

故障安全风险就是由故障的发生可能导致事故的风险。这种风险是系统最常见的风险,因此需要特别的关注。那么,由故障导致的事故会造成怎样的后果,发生的概率如何,是系统故障安全风险评价的核心。

现有的评价系统安全风险的方法大都是从风险的定义出发,通过危险的发生概率和发生的严重程度来直接度量风险。例如,董豆豆等[2]提出了在系统层面上分析系统发生事故的概率风险,但是在计算概率风险时是直接从危险源的发生后果和发生概率来计算系统的风险,并没有提出合适的评价指标,计算过程也过于简单,难以准确反映系统的风险状态。目前在国内外常采用模糊数来表示危险发生的严重程度,从而将定性的判断定量化。目前应用较多的是在航空运行管理领域[3]和铁路运行管理领域[4]。马丽仪等[5]将模糊理论与神经网络相结合,用于评价信息系统的安全风险。董国海等[6]提出了教练直升机训练系统的安全评价指标体系,将模糊理论与D-S证据理论相结合来开展对指标的评估。但是上述方法大都适用于评价指标较少的简单系统或特定的系统,而对于较为复杂的系统,由于危险的种类多,要将相应的风险评价结果集成为对系统的风险评价,则难以直接通过上述方法来实现。

因此,本文提出首先识别由故障导致事故发生的事件链,在此基础上,采用定性定量的方法对

* **收稿日期**:2014-05-04
基金项目:国家自然科学基金资助项目(71371182);高等学校博士学科点专项科研基金资助项目(20134307120026)
作者简介:蒋平(1976—),男,四川成都人,讲师,博士,E-mail:jiangping@nudt.edu.cn

事件链中后果事件的发生概率进行计算和处理，结合对发生后果的评价，最后根据上述计算结果来综合评价系统故障的风险。

系统故障安全风险评价的流程按照以下步骤逐步开展：

1）首先对系统进行结构功能分解；

2）按照系统级、分系统级、设备级分别构建其故障安全风险评价参数体系；

3）从设备级开始，由下至上逐级评价故障安全风险，最后得到系统级故障安全风险的评估结果；

4）对故障安全风险的评估结果展开分析，找出影响相应级别风险的关键因素，提出消除或者控制风险的措施；

5）在实施消除或控制措施后，再从第三步开始评价系统故障安全风险，形成一个闭环评价和降低风险的过程。

上述流程可以通过图 1 来形象描述。

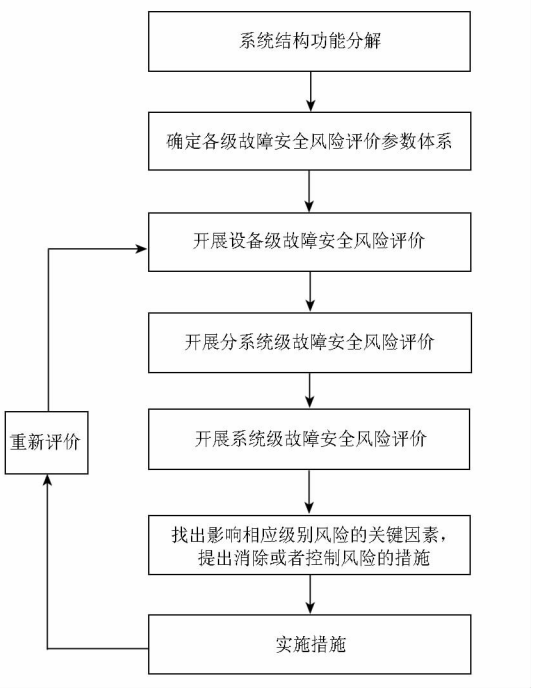

图 1 系统故障安全风险评价的流程

Fig. 1 Procedures for system failure risk evaluation

系统的故障安全风险评价可以在寿命周期内任何阶段开展，特别是在设计阶段和使用阶段，随着每一次故障安全评价的开展，风险的识别和评价得到逐步地完善，系统的故障安全风险能够得到有效的控制。

1 故障安全风险评价参数体系

根据对工程实践经验的总结，本文提出按照系统级、分系统级、设备级分别构建其故障安全风险评价参数体系。

1.1 系统级安全性评价参数

安全性风险的要求，即使用方和社会可接受的风险程度。根据系统故障安全风险评价要求，本文提出的系统级安全性评价参数为：

1）安全度

安全度是指系统在规定的时间内和规定的条件下，不发生安全事故的概率。

2）系统安全风险指数

系统安全风险指数是对系统可能发生安全事故的风险进行评价，以综合评价由分系统级的各种故障导致系统出现危险的风险大小。

这两个系统级安全性评价参数的计算方法将在 2.1 节具体介绍。

1.2 分系统级安全性评价参数

比照安全性因素分析要求，按导致事故的原因分类，分系统级的安全性评价参数可以定义为分系统级安全风险指数，对它的评价主要从物理风险、化学风险和使用风险这 3 个方面来综合开展。为了细化对分系统级安全风险指数的评价，将上述 3 个方面的风险进一步细化为 11 个评价指标，主要包括以下 3 个方面。

1）物理风险

物理风险是指可能导致事故的物理性危害因素导致的风险，主要通过以下 4 类指标来对照衡量：

①振动承受性；②温度要求；③湿度要求；④压力要求。

2）化学风险

化学风险是可能导致化学性危险的因素导致的风险，主要由易燃易爆性物质，有毒性物质、腐蚀性物质引起。主要通过以下 4 类指标来对照衡量：

①易燃性；②易爆性；③有毒性；④腐蚀性。

3）使用风险

使用风险是在系统使用过程中，由设计特性而可能引起危险的因素导致的风险。主要通过以下 3 类指标来对照衡量：

①手工操作时间；②手工操作频率；③终止危害能力。

上述部分参数在系统组成设备的安全性评价中也适用，但对于不同设备的特点，其关注的部分可能有所侧重，这会在上述参数中产生更为细致更为具体的安全性要求和参数。因此，应根据系统的危险源分析结果来确定需要评价安全性的设备，例如导弹的主要危险源为：固体火箭发动机、

战斗部、火工品等。

1.3　设备级安全性评价参数

针对火工品的安全性评价,可以参照 GJB900、GJB2236 – 92、GJB4377 – 2002、GJB2001 – 94 等标准的要求,提出可用于火工品安全性评价的参数。其他与危险源相关的设备安全性评价的参数也可参考上述标准和特定的标准提出。针对设备级产品的安全性评价已经有很多文献可以参考,这里不做具体介绍。

2　故障安全风险评价的方法

根据 1.1 节介绍的系统故障安全风险评价的流程开展风险评价工作。在已经建立了系统各级别故障安全风险评价参数的基础上对系统各级别的安全风险进行评价,找出影响各级安全的关键因素并加以控制。

2.1　设备级故障安全风险评价

设备级的安全性评价参数既有定量指标也有定性指标,这些参数的评价可以直接采用定性与定量相结合的方法来展开。

2.2　分系统级故障安全风险评价

对系统分系统级故障安全风险的评价主要通过前面提出的参数,即分系统安全风险指标来进行评价。对该参数的评价主要考虑分系统级对应的物理风险、化学风险和使用风险这 3 大类安全性评价指标及 11 个分项指标。

评价的思路是:评价按照系统的结构层次分层进行,设备级评价指标的取值可根据其自身特点选择各类评估方法来确定,例如火工品评价指标中的不发火安全电流或电压值可采用概论分布法或蒙特卡洛模拟法确定;考虑到设备级指标在确定过程中可能存在的不完备性和不确定性,分系统级评价指标的计算可根据设备级评价指标值采用模糊或粗糙集理论分析其权重矩阵,由线性或非线性加权方法确定其整体风险水平。下面采用文献[7]提出的基于粗糙集的导弹安全性评价方法,确定分系统安全性评价各分项指标的权重,再用线性加权确定分系统安全风险的评价流程。这里不再具体介绍。

由以上处理即可得到各指标的权重值 $\boldsymbol{\beta} = (\beta_1, \beta_2, \cdots, \beta_n)^{\mathrm{T}}$。最后计算分系统安全风险指数。

对分系统级的安全评价来说,可采用线性加权的形式确定

$$D = \sum_{i=1}^{n} \beta_i D_i,\ 0 \leqslant \beta_i \leqslant 1,\ \sum_{i \in S} \beta_i = 1 \quad (1)$$

式(1)中,D_i 为第 i 个评价指标离散化后的值。这里的指标离散化通过分级实现,如表 1 所示,将其分为 5 级:

表 1　安全风险指数离散化后的取值

Tab. 1　Discrete values for safety risk index

	属性离散化后的取值				
D_i	1	2	3	4	5
对应属性	弱	较弱	中	较强	强

2.3　系统级故障安全风险评价

2.3.1　对安全度的评价

由于安全度是对事故发生概率的度量,因此采用对所有识别出来的可能发生事故的概率来统计得到。具体的评价过程如下:

1)通过故障安全风险识别方法识别出那些包含系统故障事件的事件链作为分析对象。

2)对选定的每一条事件链,由引发事件开始到后果事件,采用定性估计和定量评估相结合,评价后果事件发生的可能性。对于独立事件,采用对应硬件的故障概率作为该事件的发生概率;对于相关事件,则采用 FTA(Fault Tree Algrithm)方法,由该事件的引发事件通过运算来计算该事件的发生概率。对于采用定性的评估得到的事件发生可能性,则采用模糊方法定量化,转化为事件的发生概率。

3)对事件链的后果事件按照危险来分类,对系统主要包括:爆炸、燃烧、振动等。将相同后果类型的事件链,例如所有造成爆炸事故的事件链,采用 FTA 的方法合并,合并后故障树的顶事件即系统爆炸事故,再通过故障树对顶事件发生概率的计算方法,由顶事件下面的各分支来计算该顶事件(爆炸)的发生概率。

4)综合各类危险后果的发生概率来评价系统的安全度。设识别出来的危险种类有 N 种(爆炸、机械、着火等),通过上述步骤分别计算得到各类危险的发生概率分别为 $P_i(i = 1, 2, \cdots, N)$,则系统的安全度 S 为

$$S = (1 - P_1) \times (1 - P_2) \times \cdots \times (1 - P_N) \quad (2)$$

2.3.2　对系统安全风险指数的评价

在 2.2 节对分系统安全风险指数的计算基础上,计算系统安全风险指数。计算方法如下:

设可评价风险的分系统有 N 个,按照 2.2 节可得到各分系统级的安全风险指数为 $D_1, D_2, \cdots, D_N$。由于系统级的安全风险指数与分系统级类似,是离

散化后的值,即通过表 1 的分级离散化。显然,$D_i \leqslant 5$对所有的 $i=1,2,\cdots,N$ 均成立。由于各分系统对系统安全的贡献程度不一样,定义分系统 i 的权重为 $\omega_i(i=1,2,\cdots,N)$。因此,在上述 5 级分类的条件下定义系统安全风险指数 D 为

$$D = \frac{1}{5}\sum_{i=1}^{N}\omega_i D_i \tag{3}$$

显然有 $D \leqslant 1$,该指数表示的是系统实际的安全性水平与最佳水平的差距。

2.4 系统故障安全风险评价的后续分析

风险评估通常还要在系统风险评价的基础上,寻找风险控制方法,提出降低风险的措施。因此,在上面对系统分系统级的故障安全风险评价后,需要针对评价的结果进一步开展工作。具体工作包括:

① 评价事件链中事件的重要程度,借鉴 FTA 的结构重要度概念来评价基本事件的重要程度,这里不做赘述。

② 按照事件的重要程度对故障事件排序,确定对各故障事件采取相应控制措施的先后顺序。

③ 在采取了相应的控制措施后,对事件链重新进行风险评价,即重新对系统的安全度进行评价,然后再从上面第一步重新开始评价风险,由此形成一个闭环过程,在系统寿命周期的各个阶段皆可开展故障安全风险评价。

3 系统故障安全风险评价过程示例

本文在对系统故障造成的安全性问题的辨识并建立相应的事件链的基础上,评估系统故障安全风险。

3.1 对安全度的评价

这里以某型防空导弹发生爆炸事故为例,介绍通过故障树来评价该类事故的过程以及对系统安全度的评价过程。这里在文献[8]建立的防空导弹意外点火故障树的基础上,以导弹发生爆炸为顶事件来建立故障树。所建立的故障树如图 2 所示。

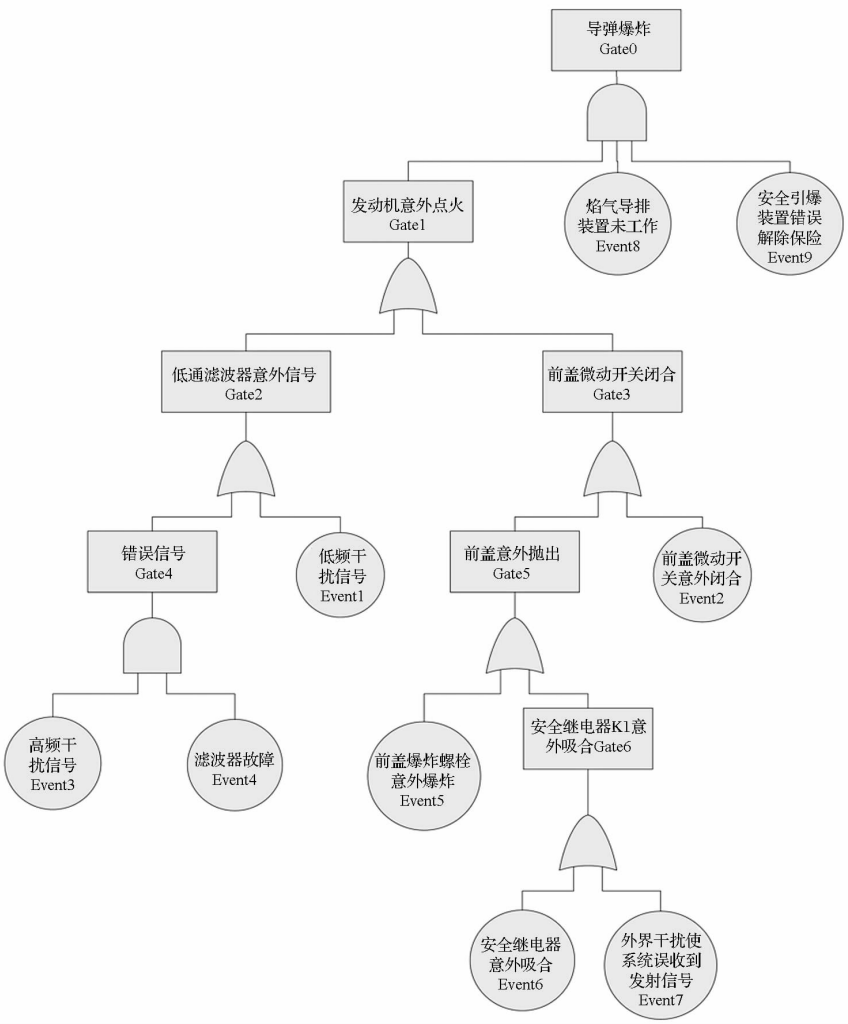

图 2 某型防空导弹爆炸的故障树

Fig. 2 Fault tree for explosion accident of an anti-air missile

3.1.1　定性分析

从故障树推导其最小割集。依据图 2 求故障树的结构式,可以得出导弹发生爆炸事故的最小割集有:$\{E_1,E_8,E_9\}$,$\{E_2,E_8,E_9\}$,$\{E_5,E_8,E_9\}$,$\{E_6,E_8,E_9\}$,$\{E_7,E_8,E_9\}$,$\{E_3,E_4,E_8,E_9\}$。这些最小割集列出了导弹发生爆炸事故的各种最基本的可能情况共有 6 种,最小割集及其代表的模式详见表 2。

表 2　导弹发生爆炸事故的模式

Tab. 2　Modes of missile explosion accident

模式	最小割集	导弹发生爆炸事故
1	$\{E_1,E_8,E_9\}$	低频干扰信号直接作用到点火器 + 焰气导排装置未工作 + 安全引爆装置错误解除保险
2	$\{E_2,E_8,E_9\}$	前盖微动开关意外闭合 + 焰气导排装置未工作 + 安全引爆装置错误解除保险
3	$\{E_5,E_8,E_9\}$	前盖爆炸螺栓意外爆炸 + 焰气导排装置未工作 + 安全引爆装置错误解除保险
4	$\{E_6,E_8,E_9\}$	安全继电器意外吸合 + 焰气导排装置未工作 + 安全引爆装置错误解除保险
5	$\{E_7,E_8,E_9\}$	外界干扰使系统误收到发射信号 + 焰气导排装置未工作 + 安全引爆装置错误解除保险
6	$\{E_3,E_4,E_8,E_9\}$	高频干扰及滤波器故障 + 焰气导排装置未工作 + 安全引爆装置错误解除保险

3.1.2　定量分析

1)基本事件发生的概率

利用前面介绍的基本事件发生概率计算方法,求得某型导弹发生爆炸事故的基本事件发生的概率,如表 3 所示。其中对涉及电子产品故障事件的发生概率是根据 GJB299B《电子设备可靠性预计手册》,对非电子类产品故障事件采用专家判断法,综合打分得到发生概率。

2)顶事件发生的概率

依据某型导弹发生爆炸事故的基本事件发生的概率,求得顶事件——某型导弹发生爆炸事故的概率为 P11 = 0.000 5。

假设由其他事件链汇总得到结果事件为典型危险事故的故障树,采用类似的方法可得发生机械事故的概率为 P2 = 0.000 3,发生振动危险的概率为 P1 = 0.000 6。

表 3　基本事件发生的概率

Tab. 3　Probabilities of basic events

序号	基本事件	发生概率
Event 1	低频干扰信号直接作用到点火器	$q_1 = 0.000\ 005$
Event 2	前盖微动开关意外闭合	$q_2 = 0.000\ 005$
Event 3	高频干扰信号干扰产生错误信号	$q_3 = 0.000\ 074$
Event 4	滤波器故障	$q_4 = 0.000\ 36$
Event 5	前盖爆炸螺栓意外爆炸	$q_5 = 0.000\ 85$
Event 6	安全继电器意外吸合	$q_6 = 0.000\ 91$
Event 7	外界干扰使系统误收到发射信号	$q_7 = 0.000\ 28$
Event 8	焰气导排装置未工作	$q_8 = 0.000\ 01$
Event 9	安全引爆装置错误解除保险	$q_9 = 0.000\ 08$

因此,可以得到系统的安全度为

$$S = (1 - P1) \times (1 - P2) \times (1 - P3) = 0.998\ 601$$

3.2　对安全风险指数的评价

根据 2.2 节的介绍,我们根据各评价指标的特点将条件属性及决策属性取值定义为 5 个级别,按由弱到强、由低到高递增的顺序划分,列表省略。

首先评价分系统的安全风险指数。假设为了评价 6 个分系统:弹体结构、动力分系统、引战分系统、弹上能源及供电分系统、电气分系统、制导及控制分系统的安全风险指数,采用专家评判,结果如表 4 所示:

表 4　专家的评价值

Tab. 4　Evaluation values from experts

分系统		S_1	S_2	S_3	S_4	S_5	S_6
权重		0.18	0.23	0.28	0.15	0.05	0.11
C	C_1	2	4	3	4	2	2
	C_2	3	5	3	4	2	3
	C_3	3	4	2	5	3	4
	C_4	5	3	3	2	4	1
	C_5	3	2	2	4	4	2
	C_6	3	4	3	2	2	4
	C_7	2	1	2	3	4	3
	C_8	2	3	2	5	4	2
	C_9	4	3	5	3	1	1
	C_{10}	3	3	4	2	1	2
	C_{11}	3	4	3	4	3	3
D 0.634		4	3	3	4	2	2

则系统的安全风险指数为

$$D = \frac{1}{5}\sum_{i=1}^{6}\omega_i D_i = 0.634$$

因此,导弹系统的安全风险指数为 0.634,偏低,存在较大的故障安全风险。

3.3 对系统故障安全风险参数评价后的分析

这里从 3.1 节的分析示例入手,目的是防止导弹爆炸事故的发生。

由 2.4 节方法得到导弹爆炸事故中各基本事件的结构重要度顺序为:

$$I_8^{st} = I_9^{st} > I_1^{st} = I_2^{st} = I_5^{st} = I_6^{st} = I_7^{st} > I_3^{st} = I_4^{st}$$

因此,相应地,应该对基本事件 8 和 9 优先采取控制措施,避免其发生;而基本事件 1、2、5、6、7 仅次于 8 和 9 采取消除或控制措施,对事件 3 和 4 的措施可以暂缓于对前面 7 个事件的控制。在采取消除或控制措施后,由于基本事件的发生概率发生了变化,应该重新对系统的安全度进行评价,再重新评价基本事件的结构重要度,从而实现对系统安全度的定量评价和闭环控制。

4 结论

目前对复杂系统的安全风险缺乏系统的评价方法,现有方法大都针对特定类型的系统开展评价,而且往往是通过直接计算系统级的评价指标来给出评价的结果,这使其难以应用于结构复杂的系统。因此,本文针对最常见的故障安全风险评价问题,提出了评价的流程,提供了从系统级、分系统级到设备级的评价参数体系和相应的评价方法,能够用于评价复杂系统的故障安全风险。

参考文献(References)

[1] 吕志彪,吴进煌,徐智明. 舰艇携行导弹使用安全性评价[J]. 战术导弹技术, 2007, 11(6): 60 - 63.
LYU Zhibiao, WU Jinhuang, XU Zhiming. Safety assessment of missile equipped for naval vessel[J]. Tactical Missile Technology, 2007, 11(6): 60 - 63. (in Chinese)

[2] 董豆豆, 周经伦, 冯静, 等. 基于概率风险的系统安全性分析[J]. 国防科技大学学报, 2005, 27(1):98 - 101.
DONG Doudou, ZHOU Jinglun, FENG Jing, et al. The analysis of system safety based on probabilistic risk[J]. Journal of National University of Defense Technology, 2005, 27(1): 98 - 101. (in Chinese)

[3] 袁乐平, 孙瑞山, 成媛. 基于模糊评价和未确知数的空管安全风险评估[J]. 中国民航学院学报, 2006, 24(4):55 - 57.
YUAN Leping, SUN Ruishan, Cheng Yuan. Fuzzy evaluation and unascertained mathematics based safety risk assessment in ATM system[J]. Journal of Civil Aviation University of China, 2006, 24(4):55 - 57. (in Chinese)

[4] 刘敬辉, 戴贤春, 郭湛, 等. 铁路系统基于风险的定量安全评估方法[J]. 中国铁道科学, 2009, 30(5):123 - 128.
LIU Jinghui , DAI Xianchun , GUO Zhan, et al. Quantitative safety assessment method based on risk in railway system[J]. China Railway Science, 2009, 30(5): 123 - 128. (in Chinese)

[5] 马丽仪, 张露凡, 杨宜, 等. 基于模糊神经网络方法的信息系统安全风险评价研究[J]. 中国安全科学学报, 2012, 22(5):164 - 169.
MA Liyi, ZHANG Lufan, YANG Yi, et al. Evaluation of information system security risk based on fuzzy neural network method[J]. China Safety Science Journal, 2012, 22(5):164 - 169. (in Chinese)

[6] 董国海, 张执国, 李晓滨. 教练直升机训练系统安全评价研究[J]. 中国安全科学学报, 2012, 22(3):115 - 121.
DONG Guohai, ZHANG Zhiguo, LI Xiaobin. Study on safety evaluation of coach helicopter training system[J]. China Safety Science Journal, 2012, 22(3): 115 - 121. (in Chinese)

[7] 江式伟, 吕卫民, 王亮. 基于粗糙集的导弹安全性评估研究[J]. 战术导弹技术, 2010, 30(3):16 - 19.
JIANG Shiwei, LYU Weimin, WANG Liang. Research on safety evaluation of the missile based on rough sets [J]. Tactical Missile Technology, 2010, 30(3): 16 - 19 . (in Chinese)

[8] 吴进煌,舰空导弹发动机意外点火故障树分析[J]. 海军航空工程学院学报, 2006, 21(6):653 - 656.
WU Jinhuang. FTA of suddenness blast-off of the engine of the ship-to-air missile[J]. Journal of Naval Aeronautical Engineering Institute, 2006, 21(6):653 - 656. (in Chinese)