

基于模糊逻辑方法的人误风险严重度识别

李鹏程^{1,2}, 陈国华², 戴立操¹, 张力¹, 赵明¹

(1. 南华大学 人因研究所, 湖南 衡阳 421001; 2. 华南理工大学 安全科学与工程研究所, 广东 广州 510641)

摘要:在系统的可靠性和安全评价中,不仅要关注硬件或软件失效引起的风险,而且要关注由人误引起的风险。本工作考虑人误可能对系统带来的风险,建立一种基于模糊逻辑方法的人误风险评价模型,识别人误风险的严重度及优先性。该方法不仅考虑人误概率,且将人误影响概率与后果严重度二因子整合到人误风险评价模型中,以满足概率风险评价的最终目的。同时,该方法能模拟系统复杂的行为历程,处理主观、模糊以及不确定的信息或知识,较传统的确定性分析方法更符合实际。通过实例说明了该方法的具体应用,表明该方法是可用的、可靠的、有价值的。

关键词:模糊逻辑;人误;风险评价

中图分类号:X928

文献标志码:A

文章编号:1000-6931(2010)05-0571-07

Fuzzy Logic-Based Approach for Identifying Criticality of Human Error Risk

LI Peng-cheng^{1,2}, CHEN Guo-hua², DAI Li-cao¹, ZHANG Li¹, ZHAO Ming¹

(1. Human Factor Institute, Nanhua University, Hengyang 421001, China;

2. Institute of Safety Science and Engineering, South China University of Technology, Guangzhou 510641, China)

Abstract: In the system reliability and safety assessment, the focuses are not only risk caused by hardware or software, but also risk caused by “human error”. This paper considers the effects of risk of human error on system, and presents a new risk assessment model of human error based on fuzzy logic used to determine risk prioritization of human error. The method not only considers the human error probability, but also integrates the error-effect probability and consequence severity into the risk assessment model to satisfy the objective of probability safety assessment. At the same time, the method can model the complex system behavior to deal with subjective, vague and uncertain information or knowledge and it is more realistic than traditional method. A case example is presented to demonstrate the proposed approach. The results show that the method is practicable, reliable and valuable.

Key words: fuzzy logic; human error; risk assessment

在人工系统的可靠性和安全评价中,不仅要关注由硬件失效引起的风险,而且还要关注由人的失误引起的风险。Trager^[1]的研究表明,核电厂中由人误引起的风险达 50%~70%。因此,减少人误是提高系统可靠性和安全的重要方面。在人工系统中,人受失误迫使条件(error-forcing conditions)的影响,易产生各种各样的失误。而每一人误均有其对应的发生概率和对系统的影响程度,如果失误发生概率高,对系统后果影响严重,那么,该人误模式即为关键人误。因此,识别关键人误及其优先性对于预防和减少人误至关重要。

现在广泛使用的第 1 代(THERP^[2]、HEART^[3])和第 2 代(CREAM^[4]、ATHEANA^[5])人的可靠性分析技术(HRA)能够给出定性和定量的分析结果。但由于现行的 HRA 存在各种各样的缺陷^[6],如数据可用性不良、专家判断的主观性、人的行为历程的复杂性等,使分析结果存在模糊性和不确定性。因此,确定性方法难以模拟现实的真实行为,而模糊逻辑方法能很好地模拟复杂的过程,处理定性的、不精确的知识和信息^[7],且在可靠性和风险评价领域有着广泛的应用^[8-11],但它们未考虑由人误带来的风险。因此,本工作采用模糊逻辑方法对系统中可能出现的人误风险严重度进行识别,并确定其优先性,为风险决策提供理论支持。

1 人误风险评价模型

本工作基于模糊近似推理建立人误风险评价模型,包括以下阶段:1)初始阶段;2)人误风险指标测量阶段;3)模糊推理阶段。

1.1 初始阶段

初始阶段包括明确具体分析对象、收集相关信息、关键任务的识别、任务分析以及人误辨识。首先是明确分析对象,即要选取有价值的分析对象并确定分析边界,本工作选择核电厂典型的极限事故作为分析对象。然后,收集和分析与选取对象相关的信息,如电厂现状、历史数据、文档文件、操作规程的分析、与有经验的专家和现场人员的访谈,以及系统结构和功能图等各种信息。关键任务的识别是识别那些有

可能对人员、财产、过程或环境造成重大损失/伤害的任务。任务分析是基于上面收集到的数据进行的分析,可采用一般的层次任务分析(Hierarchical Task Analysis, HTA),将任务分解到具体的工作任务单元,从而构建事件序列。最后,根据收集到的信息确定最有可能发生的人误。

1.2 人误风险指标测量阶段

1) 确定人误风险指标

Yu 等^[12]发展了人误严重度分析(HECA)方法,认为人误风险程度度量可通过 3 个指标来确定,即人误概率、人误影响概率和人误影响的后果严重度。假设不考虑人误风险各指标间的相对权重,则人误对系统的风险可用以下公式来表达:

$$C_{\text{HER}} = \alpha\beta\gamma \quad (1)$$

其中: C_{HER} 为人误风险严重度; α 为人误概率; β 为人误影响概率; γ 为人误的后果严重度。

2) 确定各风险指标的模糊子集或语言变量及隶属函数

为获取输入(风险指标)和输出(风险严重度)变量的不确定性及输入与输出变量间关系的不确定性知识,模糊集理论提供了描述模糊变量间近似关系的基础,用模糊集(或模糊数)来描述输入和输出特性,用隶属函数表达其不确定性。在本工作中,假设每个模糊集的隶属函数为三角形隶属函数。根据 CREAM^[4]和专家意见,人误概率用语言变量集合 HEP={非常低,低,中,高,非常高}来表示(表 1)。

3) 每个人误风险指标的测量

分析人员或专家需根据其知识和经验来测量每个可能发生的人误所对应的风险指标。由于受主观因素的影响(如获取信息的完备性、知识差异等),专家或分析人员给出的测量结果可能是一精确值,也可能是范围值、模糊数或语言值。由于模糊推理系统需输入精确值,因此,对于上述不精确的测量结果,通过三角形重心解模糊的方法求解:

$$F_i = \frac{(u_i - l_i) + (m_i - l_i)}{3} + l_i \quad (2)$$

如人误后果评价为“非常低”,则由三角形重心解模糊法得到的精确值为 0.083。

表 1 人误风险指标的语言变量及模糊集
Table 1 Linguistic variables and fuzzy sets of risk indices of human error

等级	语言变量	人误概率	语言变量	人误影响概率	后果严重度	损失百分比
1	非常低(V-L)	$0.5 \times 10^{-5} \leq \alpha < 1 \times 10^{-3}$	几乎无影响(A-N-E)	$0 \leq \beta < 0.05$	非常低(V-L)	$0 \leq \gamma < 0.25$
2	低(L)	$1 \times 10^{-4} \leq \alpha < 1 \times 10^{-2}$	有可能(possible-E)	$0 \leq \beta < 0.55$	低(L)	$0 \leq \gamma < 0.5$
3	中(M)	$1 \times 10^{-3} \leq \alpha < 1 \times 10^{-1}$	很有可能(probable-E)	$0.05 \leq \beta < 1$	中(M)	$0.25 \leq \gamma < 0.75$
4	高(H)	$1 \times 10^{-2} \leq \alpha < 0.5$	绝对有影响(A-E)	$0.55 \leq \beta < 1$	高(H)	$0.5 \leq \gamma < 1$
5	非常高(V-H)	$1 \times 10^{-1} \leq \alpha \leq 1$			非常高(V-H)	$0.75 \leq \gamma \leq 1$

1.3 模糊推理阶段

在人误风险推理阶段,风险分析人员将确定的人误概率、人误影响概率及人误后果的严重度输入模糊推理系统,通过模糊化分别转化为相匹配的模糊集。将这些模糊集输入模糊推理系统,激活相关的模糊规则,再通过解模糊计算人误风险度精确地输出结果。

1) 建立模糊推理系统

模糊逻辑最初是由 Zadeh^[13]以一种数学的方式来描述生活中的模糊现象,模糊逻辑系统的近似推理功能胜于精确推理。模糊逻辑与传统的模拟技术相比,其基本的差异是集合的定义。传统的集合理论是二值逻辑,表达“非此即彼”的现象,而模糊逻辑中定义的集合是模糊集,它无明确的边界,表达存在现实中的“亦此亦彼”的现象,特别是表达事物模糊性的重要概念——隶属函数的引入,才能对所有的模糊概念进行定量表示^[14-15]。模糊推理过程包括 4 个基本组成部分,即模糊规则库、模糊推理过程、模糊化过程以及解模糊过程^[9,11,16]。可采用 Matlab7.0 中的模糊逻辑工具箱来构建模糊推理系统^[15]。在构建系统前,必须确定输出变量(风险严重度)的模糊集以及模糊规则。

(1) 确定输出变量的模糊集合

根据文献[10]和专家意见,人误风险严重度用语言变量集合 HERC={几乎没有,微小,非常低,低,中,高,中高,非常高,极高,绝对高}来表示,共分为 10 个等级。图 1 是其图形化表征。

(2) 发展连接输入和输出变量的模糊规则库

模糊规则是用 IF-THEN 的形式建立人误概率、影响概率及后果严重度 3 个指标与风险输出间语言值的联系,通过专家讨论得到的指

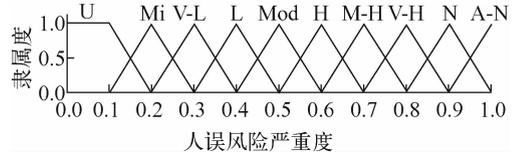


图 1 人误风险严重度的模糊集(隶属函数)
Fig. 1 Fuzzy sets (Membership function) for risk criticality of human error

标的隶属函数及风险的指标函数被用于产生模糊规则库(假设 3 参数同等重要)。根据专家意见,对每个输入参数的多个模糊集采用逻辑“与”操作,使模糊规则库中总规则可达 100 个(5×4×5)。现给出一些规则如下。

规则 1: 如果人误发生概率是“非常低”,失误影响概率是“几乎没有影响”,人误后果严重度是“非常低”,则风险严重度是“几乎没有”。

规则 33: 如果人误发生概率是“高”,失误影响概率是“有可能”,后果严重度是“非常低”,则风险严重度是“低”。

规则 67: 如果人误发生概率是“非常低”,失误影响概率是“有影响”,后果严重度是“非常高”,则风险严重度是“中高”。

规则 93: 如果人误发生概率是“高”,失误影响概率是“有影响”,后果严重度是“高”,则风险严重度是“极高”。

有了这些模糊的 IF-THEN 规则,即可将模糊输入转化成模糊输出。

2) 识别人误风险的优先性

通过模糊推理系统的输出,可得到每个人误风险的严重度结果,从而可识别它们之间的风险优先性和重要性。输出的结果必须经审核,如果在输出结果中发现一些不合理的现象,必须找到原因,对输入参数进行修订,重新评价风险推理过程,最终对输出结果进行修正,得到

可靠性数据,以利于风险决策。

2 案例分析

在核电厂始发事件后,受各种情境环境的影响,操纵员的响应可能产生失误。本工作选用压水堆核电站蒸汽发生器传热管断裂(SGTR)事故为例说明该方法的具体应用^[6]。

2.1 初始阶段

1) 明确分析对象并收集相关信息

SGTR事故是指在1台蒸汽发生器中发生1根或两根传热管断裂的事故,其特性是一回路压力边界完整性遭到破坏,使得一回路冷却剂通过破损蒸汽发生器向二回路泄漏。因此,需及时隔离破损蒸汽发生器,以便终止放射性向外泄漏,并通过降温、降压、安注等处理,最终将机组带到冷停堆工况。操纵员在这一系列处理过程中,可能出现各种各样的失误,如果失误发生,则有可能对系统和环境造成影响。然后,收集与对象相关的信息,如电厂最终安全分析报告、管路系统流程图、电气系统图和仪表系统图等。

2) 识别关键任务并进行详细的任务分析

在发生SGTR事故后,本工作以成功隔离破管SG为分析对象,根据专家意见、收集的信息、层次任务分析原理及电厂的紧急操作规程(EOP),构建事件序列(表2)。

3) 识别可能的人误

许多人误辨识技术可用于识别可能发生的人误,本工作选取第2代HRA方法——CREAM,它是考虑情境环境对人的认知和行为影响的典型代表。详细的人误识别过程参见文献[4]。基于CREAM识别的可能发生的人误模式列于表2。

2.2 人误风险指标测量阶段

1) 确定人误概率

依据CREAM方法,人误概率可通过以下步骤确定:(1)确定每个失误模式基本的或名义上的失误概率;(2)评价情境环境对失误的影响,对名义上的失误概率进行修订;(3)调整失误概率,获得修正后的失误概率。

2) 确定失误影响概率

失误影响概率是假设某个失误已发生,识别该失误对系统产生某种已识别的等级影响发

生的可能性。它是一种条件概率,亦即失误影响概率是确定某失误发生后对系统产生某种程度影响的置信度。例如,在子任务1.1中,可能的人误模式为O3,导致系统损失的等级被评价为“非常低”,失误影响概率为1。这意味着绝对相信如果发生人误模式O3将100%引起“非常低”等级的系统损失。

3) 确定人误的后果严重度

人误影响硬件系统、系统功能和人员安全等。可从安全、可靠性、维修性、质量、损失等方面来综合考虑确定后果严重度等级。本工作假设人员的认知失误影响存在,且在反应过程中,如诊断失误,肯定会影响操作失误,从而判断心理认知错误对系统的影响,可根据其对下一行为动作错误的影响来评价。

现以子任务1.1发觉异常报警信号来说明人误风险指标的测量。根据CREAM,子任务1.1所需的认知行为为观察,认知功能也为观察,可能出现的认识失误为“O3——观察错过”,其基本的失误概率为0.007,根据电厂实际情况,评估9个CPCs(共同绩效条件)的状态,得到总的权重因子为0.128(表3)。然后,对基本的失误概率进行修订,得到修订后的概率为0.000896。再确定发生该失误对系统可能造成的影响后果,评估为“非常小”,采用三角形重心解模糊法得确切值为0.083。最后,判断该失误影响发生的可能性,由于会对后续行为产生影响,故评估其概率为1。同理,可分析其余的子任务,指标的测量结果同列于表2。

2.3 模糊推理阶段

将每个人误的3个风险指标的测量值分别输入到建立的模糊推理系统中(人误概率值需经对数处理才能输入到推理系统中)。如子任务1.1的失误概率0.000896对数处理后为-3.0477(表2括号中的数值),失误影响概率为1,失误后果严重度为0.083,输入模糊推理系统,得到该人误的风险严重度为0.429。同理可得其它人误的风险严重度输出结果(表2)。通过专家对表2的审核,不存在奇异结果。因此,由表2可知,最严重的失误模式是子任务1.2中的I1和2.2中的I2,其风险值达0.798,这主要是因诊断属知识型行为,发生失误的概率高,如果诊断错误,便会产生蒸汽发生器破管

表 2 隔离破损 SG 的任务步骤及风险识别结果
Table 2 Steps in isolation of damaged SG and results of risk assessment

任务	子任务	认知行为	认知功能	可能失误	名义失误概率	权重因子	调整后的概率	失误影响	失误影响等级 (确切值)	后果严重程度 (确切值)	人误风险严重程度
1 停堆或安全注	1.1 发觉电厂异常状态或报警信号 (N16 高报)	观察	观察	O3	0.007	0.128	0.000 896(-3.047 7)	反应在过程中	1	V-L(0.083)	0.429
	1.2 识别警报类型、严重程度及性质	识别	解释	I1	0.02	0.1	0.002(-2.699)	选择错误规程	1	V-H(0.916 7)	0.798
	1.3 确定停堆	评估	解释/计划	I1	0.02	0.1	0.002(-2.699)	重新确认	Probable-E (0.533 3)	L(0.25)	0.429
	1.4 确认系统/组件状态及可用性	确认	观察/解释	O3	0.007	0.128	0.000 896(-3.047 7)	出现潜在故障	1	H(0.75)	0.697
2 识别并隔离破损的 SG	2.1 检查主系统压力	A. 观察	观察	O3	0.007	0.256	0.001 792(-2.746 7)	反应在过程中	Probable-E (0.533 3)	M(0.5)	0.524
		B. 评估	解释/计划	I1	0.02	0.2	0.004(-2.397 9)	反应在过程中	Probable-E (0.533 3)	M(0.5)	0.553
	2.2 识别破损的 SG	A. 观察	观察	O2	0.007	0.256	0.001 792(-2.746 7)	反应在过程中	1	V-H(0.916 7)	0.793
		B. 诊断	解释/计划	I2	0.01	0.2	0.002(-2.699)	放射性外泄	1	V-H(0.916 7)	0.798
2.3 隔离破损的 SG	2.3.1 调整破损 SG 的大气释放阀开启设定值 7.0 MPa	A. 监视	观察/解释	O3	0.007	0.256	0.001 792(-2.746 7)	主系统高压	1	H(0.75)	0.729
		B. 调整	观察/执行	E1	0.003	0.204 8	0.000 614 4(-3.211 5)	主系统高压	1	H(0.75)	0.687
	2.3.2 确认破损 SG 的大气释放阀——关闭	确认	观察/解释	O3	0.007	0.256	0.001 792(-2.746 7)	反应在过程中	Probable-E (0.533 3)	H(0.75)	0.624
	2.3.3 关闭破损 SG 的主蒸汽隔离阀及其旁路	执行	执行	E3	0.000 5	0.204 8	0.000 102 4(-3.989 7)	放射性外泄	1	H(0.75)	0.602
2.3.4 隔离破损 SG 的排污	2.3.4 隔离破损 SG 的排污	执行	执行	E3	0.000 5	0.204 8	0.000 102 4(-3.989 7)	降低安全功能	1	L(0.25)	0.402
	2.3.5 关闭破损 SG 的主蒸汽隔离阀前疏水	执行	执行	E3	0.000 5	0.204 8	0.000 102 4(-3.989 7)	降低安全功能	1	L(0.25)	0.402
2.4 确认隔离成功	核实	观察/解释	O2	0.007	0.256	0.001 792(-2.746 7)	反应在过程中	Probable-E (0.533 3)	V-L(0.083)	0.357	

表3 评价CPCs对认知功能失效的影响权重
Table 3 Assessment of effects of CPCs on cognitive function failures

CPC	子任务 1.1	权重因子
组织的充分性	非常有效	1
工作环境	有利的	0.8
MMI 和操作支持的充分性	充分的	1
规程/计划的可用性	充分的	0.8
需同时响应的目标数量	与能力匹配的	1
可用时间	充分的	0.5
工作时段	白班	1
培训、准备的充分性	充分的且有相当的经验	0.8
员工的协作质量	十分有效的	0.5

0.128(总权重因子,各因子积)

隔离不成功,其后果也相当严重。其次的失误模式是子任务 2.2 中的 O2,其风险值达0.793,这些失误模式是电厂首先考虑预防的人误。接下来,人误风险严重度依次为任务 2.3.1 中的 O3,子任务 1.4 中的 O3 等。因此,组织可根据获得的数据有针对性地采取措施预防人误的发生。

2.4 传统的 HECA 与本工作提出的 FHECA 方法的比较分析

分别采用 HECA 与 FHECA 对人误风险进行分析,得到的结果列于表 4。由表 4 可知,前 3 位排序无变化,但第 4 位排序开始有所变化,子任务 1.4 确认系统/组件的状态及可用性与子任务 2.1.2 评估主系统压力相比,对于系统损失和安全,子任务 1.4 比子任务 2.1.2 更为重要,如果未能确认系统状态/组件的可用性,系统可能产生潜在的故障,在后续动作执行后,会触发不利的后果。相反,子任务 2.1.2 评估主系统压力是否出错,主要影响的是否停主泵对后续行为和系统的影响相对较小。另外,对于任务 1.1 发觉电厂异常状态或报警信号和子任务 1.3 确定停堆,HECA 分析的结果排序不同,这是因传统方法相对放大了人误概率的风险贡献。但由 FHECA 分析的结果排序相同,主要是因基于假设“电厂一般都会自动停堆成功”,故它们对系统带来的风险是一致的,这更符合实际。同理可分析其它变化的排序结果。因此,在缺少信息和证据的条件下,模糊逻辑方法更能模拟真实的系统行为。

表4 HECA 与 FHECA 分析人误风险结果的比较

Table 4 Comparison of analytical results between HECA and FHECA

任务序号	HECA 结果	FHECA 结果	HECA 排序	FHECA 排序
1.1	0.000 074 4	0.429	12	10
1.2	0.001 833 4	0.798	1	1
1.3	0.000 266 7	0.429	9	10
1.4	0.000 672	0.697	6	4
2.1(A)	0.000 477 8	0.524	7	9
2.1(B)	0.001 066 6	0.553	4	8
2.2(A)	0.001 642 7	0.793	2	2
2.2(B)	0.001 833 4	0.798	1	1
2.3.1(A)	0.001 344	0.729	3	3
2.3.1(B)	0.000 460 8	0.687	8	5
2.3.2	0.000 716 8	0.624	5	6
2.3.3	0.000 076 8	0.602	11	7
2.3.4	0.000 025 6	0.402	13	11
2.3.5	0.000 025 6	0.402	13	11
2.4	0.000 079 3	0.357	10	12

3 结论和讨论

1) 基于模糊逻辑的人误风险严重度识别方法很好地模拟那些复杂的行为,处理不精确的、模糊的和不确定性的数据和信息,不仅能识别人误风险的优先性,而且能识别人误风险的重要性。

2) 该方法将失误影响概率和后果严重度

两个指标整合到风险评价模型中,克服了现存的人的可靠性分析技术(如 THERP、CREAM)等过度强调人误概率的计算、忽视失误影响概率和后果严重度评价、未达到概率安全评价的最终目的的缺陷。

3) 考虑到人误概率的确定、人误的影响概率及人误后果严重度的确定均带有专家的主观判断和不确定性,因此,由 HECA 与 FHECA 分析结果的比较可知,采用 FHECA 进行人误风险严重度识别可使分析结果更可靠,尽力避免误导,便于组织做出正确的风险决策。

但在建立模糊规则库中,本工作将人误的 3 个风险指标权重视为同等重要,这在现实中是不存在的。同时未考虑失误恢复,结果计算偏于保守。因此,合理确定 3 个风险因子权重以及合理考虑失误恢复而使研究结果更为可靠是下一阶段的研究工作。

参考文献:

- [1] TRAGER T A. Case study report on loss of safety system function events, AEOD/C504 [R]. Washington D. C. : US Nuclear Regulatory Commission, 1985.
- [2] SWAIN A D, GUTTMANN H E. Handbook of human reliability analysis with emphasis on nuclear power plant applications, NUREG/CR-1278 [R]. Washington D. C. : Sandia National Laboratories, 1983.
- [3] WILLIAMS J C. Toward an improved evaluation tool for users of HEART [C] // Proceedings of the International Conference on Hazard Identification, Risk Analysis, Human Factors and Human Reliability Process Safety. Orlando: Chemical Centre for Process Studies (CCPS), 1992: 261-271.
- [4] HOLLNAGEL E. Cognitive reliability and error analysis method [M]. Oxford (UK): Elsevier Science Ltd., 1998.
- [5] COOPER S E, RAMEY-SMITH A M, WREATHALL J. A technique for human error analysis, NUREG/CR-6350[R]. Washington D. C. : USNRC, 1996.
- [6] 张力. 概率安全评价中人因可靠性分析技术 [M]. 北京:原子能出版社,2006.
- [7] KLIR J, YUAN B. Fuzzy sets and fuzzy logic: Theory and applications[M]. New Jersey: Prentice Hall, 1995.
- [8] BOWLES J B, PELAEZ C E. Fuzzy logic prioritization of failures in a system failure mode, effects and criticality analysis[J]. Reliability Engineering and System Safety, 1995, 50: 203-213.
- [9] YADAV O P, SINGH N, CHINNAM R B, et al. A fuzzy logic based approach to reliability improvement estimation during product development [J]. Reliability Engineering & System Safety, 2003, 80: 63-74.
- [10] GUIMARAES A C F, LAPA C M F. Fuzzy inference to risk assessment on nuclear engineering systems[J]. Applied Computing, 2007, 7: 17-28.
- [11] KONSTANDINIDOU M, NIVOLIANITOU Z, KIRANOUDIS C, et al. A fuzzy modeling application of CREAM methodology for human reliability analysis[J]. Reliability Engineering & System Safety, 2006, 91: 706-716.
- [12] YU F J, HWANG S L, HUANG Y H. Task analysis for industrial work process from aspects of human reliability and system safety[J]. Risk Analysis, 1999, 19(3): 401-415.
- [13] ZADEH L A. Fuzzy sets[J]. Inform Control, 1965, 8: 338-352.
- [14] 杨纶标,高英仪. 模糊数学:原理及应用[M]. 广州:华南理工大学出版社,2003.
- [15] 闻新,周露,李东江,等. Matlab 模糊逻辑工具箱的分析与应用[M]. 北京:科学出版社,2002.
- [16] 王士同. 模糊推理理论与模糊专家系统[M]. 上海:上海科学技术文献出版社,1995.