第 29 卷 第 5 期
2003 年 9 月

自 动 化 学 报
ACTA AUTOMATICA SINICA

Vol. 29, No. 5
Sept., 2003

基于有向图故障树自动建树方法的规范化描述及其应用研究[1)]

钱彦岭　　邱　静　　温熙森

（国防科技大学机电工程研究所　长沙　410073）

（E-mail: diagnosis@nudt.edu.cn）

摘　要　基于有向图的建树方法是目前故障树自动建树研究中最常用的方法之一，但其有效性多年来一直存在争议，其主要原因在于采用传统的专家定义的算子进行建树推理时，算子定义不规范，导致对系统复杂的控制结构适应能力不强. 该文利用人工智能的原理，对定性推理逻辑进行了必要的扩展，提出了建树过程的形式化描述，在此基础上将故障树的建树问题转化为一个约束满足问题(CSP)，从而可利用比较成熟的算法来解决上述问题. 针对实际问题的例证说明了这一过程. 研究表明，文中所提出的方法更便于计算机自动处理，减少建树过程中的人为失误，可有效地提高故障分析效率.

关键词　故障树自动建树，多值逻辑，约束满足问题

中图分类号　TB114

Research on Formal Description of Digraph-Based Fault Tree Construction and Its Application

QIAN Yan-Ling　QIU Jing　WEN Xi-Sen

(*Institute of Mechatronic Engineering, National University of Defense Technology, Changsha*　410073)

(E-mail: diagnosis@nudt.edu.cn)

Abstract　As one of the most attractive approaches in fault tree automatic construction, the digraph-based fault tree construction is not effective for complex system due to the unsuitable traditional operators defined by domain experts. In this paper, a formal description of the construction process is developed by extending the multiple-valued logic and utilizing constraint logic programming principle. Thus, the fault tree construction is transformed to a constrain satisfaction problem (CSP). And the problem can be simply solved through the CSP algorithms. The results of the fault tree automatic construction for a classical example show our method can reduce inaccuracy and is more efficient and effective.

Key words　Fault tree automatic construction, multiple-valued logic, constraint satisfactory problem

1) “九五”国防预研项目资助
Supported by the “Jiu-Wu” National Defense Preparatory Research Projects

收稿日期　2001-04-26　　收修改稿日期　2002-09-10
Received April 26, 2001; in revised form September 10, 2002

1 引言

在复杂系统的可靠性设计与分析[1]、故障诊断[2]和测试性设计[3]中,故障树分析法的应用十分广泛.但是,故障树的建造通常仍采用手工方法进行,效率低、费用高,发生遗漏和错误不可避免.因此,故障树的自动建造已成为人们的研究重点之一[4],其中基于有向图法的自动建树方法受到了重视[5~8],但有向图法的建树推理过程通常采用自然语言定义的算子[9~11],规范性差,在处理复杂系统结构时,会造成建树结果产生偏差.本文在这方面作进一步改进,提出了建树过程的规范化描述,将其转化为一个约束满足问题(Constraint Satisfactory Problem,CSP)[12]进行求解.

2 系统的有向图描述及基于有向图的故障传播关系

按照系统论的观点[13],系统由部件(子系统)、系统结构功能关系、系统所处环境三部分组成,系统的功能可通过输入输出变量来体现,这种思想可用有向图形式描述[14].

系统的功能模型可用有向图 $G=G(V,E,W)$ 表示,其中节点集 V 表示系统中的过程变量或事件;边集 E 中的边用来连接具有因果关系的两个节点,边的方向由独立变量指向相关变量,每条边都有相应的数值,称作增益,表示变量之间关系的强度;有向图 G 中所有增益用权矩阵 W 表示.有向图的边可分为两类[10]:正常边和异常边,正常边是指系统功能正常时变量之间关系成立的边;异常边是指在一定异常条件下变量之间关系成立的边.当同一节点对之间存在多条边时,在系统运行的某一时刻,只有一类边定义的关系成立.正常边和异常边分别描述了系统在正常情况和故障情况下变量之间的关系.

根据功能模型,系统故障可看作是输出变量偏离正常值或输入输出变量间正常功能关系的改变.为便于故障分析,变量的值采用定性表示,将变量所有可能发生的偏差与其正常值相比,当偏差很大超出控制范围无法完全补偿时,用 ± 10 表示;当偏差中等可被控制系统补偿时,用 ± 1 表示;参数取值正常时用 0 表示.故障信号通过变量间的相互关系即增益系数在系统中传播,根据变量之间关系的强弱,同样将增益系数用定性数值 ± 10,± 1 和 0 表示.

在有向图模型中,表示过程变量的节点叫做过程节点,表示某个失效事件的节点叫做失效节点.一条有向边的头部节点叫做该边的原因节点,其尾部节点即该边所指向的节点,称为该边的结果节点.过程节点对应的变量叫做过程节点变量,失效节点和有向图的边定义的条件所对应的变量叫做失效变量.对过程变量和失效变量的取值,约定如下:过程变量的取值为 ± 10,± 1 或 0;失效变量是布尔变量,其取值为 0 或 1,当失效变量取 0 时表示相应的失效事件没有发生,当失效变量取 1 时表示相应的失效事件已经发生.

为对复杂系统进行合理建树,首先必须研究系统中故障的传播关系.根据有向图模型,故障的传播实际上是变量的偏差信号通过有向图的边在系统中的传播,根据多值逻辑[14]理论,我们可以得到有向图中两变量之间的运算关系满足表 1 确定的 5 值逻辑关系,其中 u 代表不能确定.

表 1　故障传播关系表

Table 1　Relationship of fault propagation

B \ A	+10	+1	0	−1	−10
+10	+10	+10	0	−10	−10
+1	+10	+1	0	−1	−10
0	0	0	0	0	0
−1	−10	−1	0	+1	+10
−10	−10	−10	0	+10	+10

$A\times B$

B \ A	+10	+1	0	−1	−10
+10	+10	+10	+10	+1/+10	*u*
+1	+10	+1	+1	0	−1
0	0	+1	0	−1	−10
−1	+1	0	−1	−1	−10
−10	*u*	−1/−10	−10	−10	−10

$A+B$

表 1 中定义的 5 值逻辑关系和传统的多值逻辑[5]是有区别的，主要原因在于建模时假定±1 偏差可以被系统补偿、±10 偏差不可完全补偿. 当+10(−10)和−1(+1)相加时，若系统功能正常，结果为+1(−1)，表示大的偏差经过补偿变为中等偏差，若系统失效，结果为+10(−10)，表示故障偏差不可补偿；当+1(−1)和−1(+1)相加时为 0，表示中等偏差经过补偿偏差抵消. 利用这种运算规则，变量的加法不再满足结合率，为此，在功能模型中，构造多变量的加法按下式进行

$$\sum x_i = \left(\sum A_j\right) + \left(\sum B_k\right) \tag{1}$$

式中 A_j 是变量集$\{x_i\}$中符号为正的项，B_k 是$\{x_i\}$中符号为负的项. 式(1)的物理意义在于，变量的求和实际上是不同性质(符号)的变量互相作用的结果，同种性质的变量对变量和的作用趋势相同，应优先处理.

对于系统功能模型中的一个结果过程节点，如果没有负反馈环与之相关，则其对应过程节点变量可由下式确定

$$EN = \sum CN \times w \tag{2}$$

式中 EN 表示某结果过程节点“EN”相应的过程节点变量，CN 表示 EN 的原因节点变量，w 是CN 与EN 之间的增益值. 当两相邻节点同时存在正常边和异常边时，节点之间的权值按下式计算

$$w_{ij} = \sum_{l=1}^{K} w_l \cdot e_l \prod_{h=1,h\neq l}^{K} \overline{e_h} \tag{3}$$

式中 K 是两相邻节点 v_i和 v_j之间边的总数，e_l是边定义的失效变量. 式(3)保证了相邻节点之间只有一条边成立. 式(2)只有在节点“EN”不和负反馈环相关时才能成立，这是由于负反馈环对中等偏差具备调节消除的作用，直接利用式(2)和表 1 通常会得出矛盾的结论. 为体现反馈环的作用，通常要引入环变量的概念[6, 12].

设系统的功能模型 $G=G(V,E,W)$，给定节点 $v_i\in V$，存在回路 $v_1e_1v_2e_2\cdots v_ne_n$，且$w(e_1)\times w(e_2)\times\cdots\times w(e_{n-1})<0$，则称该回路是负反馈环，其中 $w(e_i)$是环路中节点 v_{i-1}，v_i之间正常边的权值. 对于每一个负反馈环，定义一个变量与之对应，称为环变量. 环变量等于负反馈环中各段增益之积，即

$$LOOP = \prod w_{\text{loop}} \tag{4}$$

其中 $LOOP$ 为环变量，w_{loop}为环中相邻两节点之间的增益. 如果回路中某个节点 v_i是该反馈环控制元部件的输出节点，则称与 v_i反馈环相关，此时，节点参数取值为[5]

$$EN = J\times\sum LOOP + \sum DCN\times G \tag{5}$$

上式中 EN 是与过程节点“EN”相关的负反馈环的环变量；DCN 是进入反馈环的外部扰动节点变量；G 是外部扰动“DCN”传播到“EN”的路径上各边的边增益之积；J 是环变量的符

号因子,表示负反馈控制环正常时的调整方向,定义为

$$J=\begin{cases}+1, & EN>0,\ LOOP<0\\ -1, & EN<0,\ LOOP<0\\ +10, & EN>0,\ LOOP>0\\ -10, & EN<0,\ LOOP>0\end{cases}\tag{6}$$

上述约定同时描述了反馈环正常作用时和反馈环失效时的功能关系:当反馈环正常作用时,对进入环路的偏差具有校正作用;当反馈环由于环路构成元件的特性转变成正反馈时,系统输出产生较大的偏差.

3 故障树自动建树算法

在进行故障树分析时,需首先假定某个过程节点的偏差值,并研究造成该偏差值的所有因素.根据上面定义的变量的取值关系,容易将故障树建树问题等效为一个约束满足问题(Constraint Satisfaction Problem,CSP)[12].一个典型的 CSP 问题包括:1)变量集 $X=\{x_1,x_2,\cdots,x_n\}$; 2)每个变量 $x_i\in X$ 对应的定义域 D_i,它们是有限域;3)约束集 $C=\{c_1,c_2,\cdots,c_m\}$,限定变量可以同时取的值.

CSP 问题的求解目标为给定变量的定义域和约束条件(约束集),求满足条件的变量集合.这样,给定系统控制元件输出过程节点 EN 的输出偏差值,可以构造下面的 CSP 问题,不失一般性,假设该过程节点与反馈环相关,有

- 变量集 $X=P\cup F$;
- 变量定义域,对于每个 $x_i\in P$,$x_i\in\{-10,-1,0,1,10\}$, $x_i\in F$, $x_i\in\{0,1\}$;
- 约束集 $EN=J\times\sum LOOP+\sum DCN\times G$, $EN=Dev$.

其中 P 和 F 分别是所有与节点变量表达式 EN 相关的过程节点变量和失效变量,Dev 是设定的偏差值.针对 CSP 问题,已经提出了很多求解算法,典型的有生成-测试算法(Generate-Test Algorithm,GT)[12].由此,参照文献[5],构造自动建树算法如下:

① 建立系统有向图功能模型并定义顶事件;

② 将顶事件压入堆栈;

③ 若堆栈为空,则故障树建造完毕;非空,从堆栈中弹出一个事件作为当前事件并置其变量为当前变量;

④ 由式(2)~(6)列写节点变量的关系式;

⑤ 利用 GT 算法、表 1 和式(1)求解满足约束条件的解;由解作相应故障树枝;

⑥ 将非底事件压入堆栈,转④.

4 应用实例及结论

根据本文提出的形式化定义和算法,我们研究由 Lapp 和 Powers 提供的硝酸冷却器例子[8](图 1).热硝酸通过由冷水泵控制的开关阀,进入热交换器,和由冷水泵泵入的冷水进行热交换,冷却后的硝酸由温度传感器进行测量,控制冷水的流量,使硝酸控制在一定的温度范围内.冷却器的有向图模型如图 2 所示.由图中 $T3$,$P6$,$P7$ 和 $M8$ 形成负反馈环,$T3$ 是控制元部件的输出节点,由式(5)可得

$$T3=M2+T2+P9\times(-1)+T8+EF4\times[\overline{VR5}+VR5\times(-1)]\times(-1)+$$

$$LAP\times(\overline{VR5}+VR5\times(-1))+LOOP1\times J+EF2,$$

$$LOOP1=-\overline{SB}\times[(\overline{CB}\times\overline{CAR})+CAR\times\overline{CB}\times(-1)]\times[\overline{VR5}+VR5\times(-1)].$$

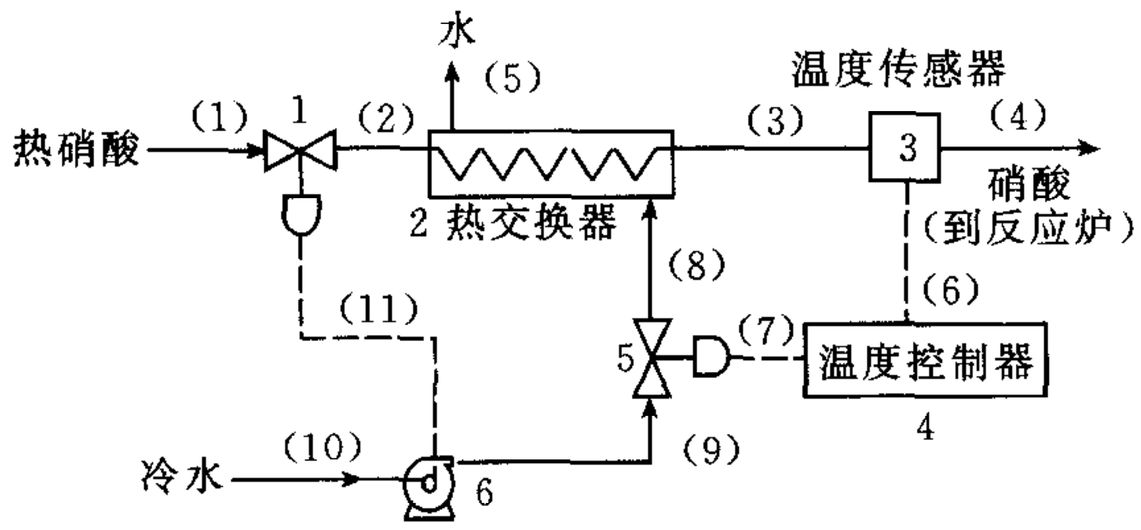

图 1　硝酸冷却器结构示意图

Fig. 1　Diagram of nitric acid cooler

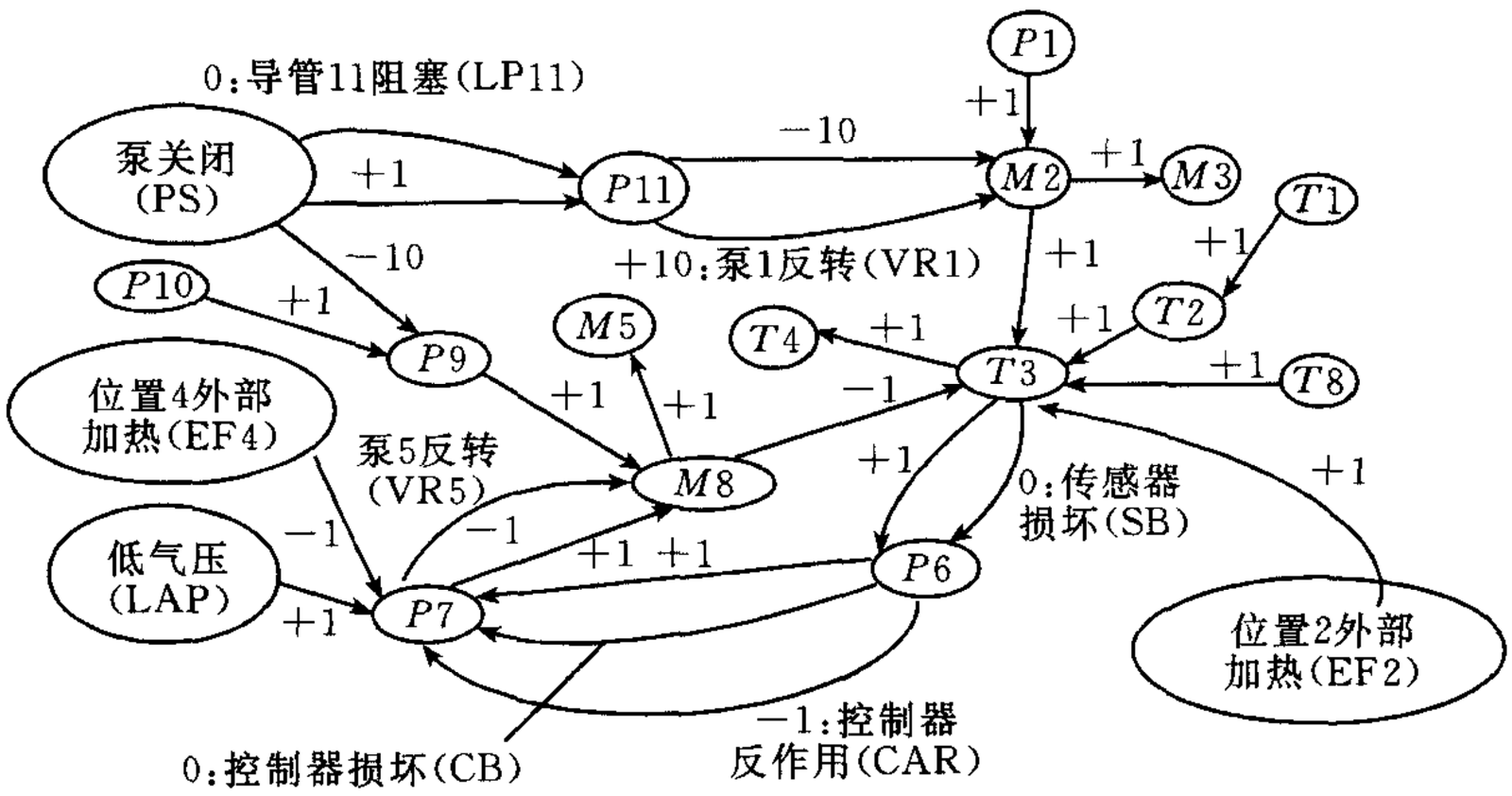

图 2　硝酸冷却器有向图模型

Fig. 2　Diagraph of the nitric acid coodler

由式(5)～(7)可知，当环路正常作用时，进入的偏差 $P9$，$T2$，$M2$ 或 $T8$ 出现微小扰动时，$T3$ 没有偏差，即冷却器输出的硝酸温度是恒定的；当 $P9$，$T2$，$M2$ 或 $T8$ 偏差较大超过反馈环的补偿范围时，硝酸温度出现一定的偏差；当泵 5 或温度控制器 4 特性反转使反馈环变成正反馈时，导致硝酸温度越高泵 5 流经的冷水量越小，使硝酸温度产生较大的偏差. 设 $T3$ 出现中等偏差为顶事件，构造 CSP 问题如下：

变量集 $X=\{M2,\ P2,\ P10,\ PS,\ VR5,\ LAP,\ SB,\ CB,\ EF2,\ CAR\}$；定义域 $M2$，$P2$，$P10\in\{-10,-1,0,+1,+10\}$，$PS$，$VR5$，$LAP$，$SB$，$CB$，$CAR\in\{0,1\}$；约束集 $T=-1$. 利用 GT 算法，可以求出满足约束条件的变量集合为：当 $LOOP=-1$ 时，$M2=+10$ 或 $P9=-10$ 或 $T8=+10$ 或 $T2=+10$；当 $LOOP=0$ 时，$LAP=1$ 或 $EF2=1$，$M2=+1$ 或 $P9=-1$ 或 $T8=+1$ 或 $T2=+1$. 由解得故障树如图 3 所示.

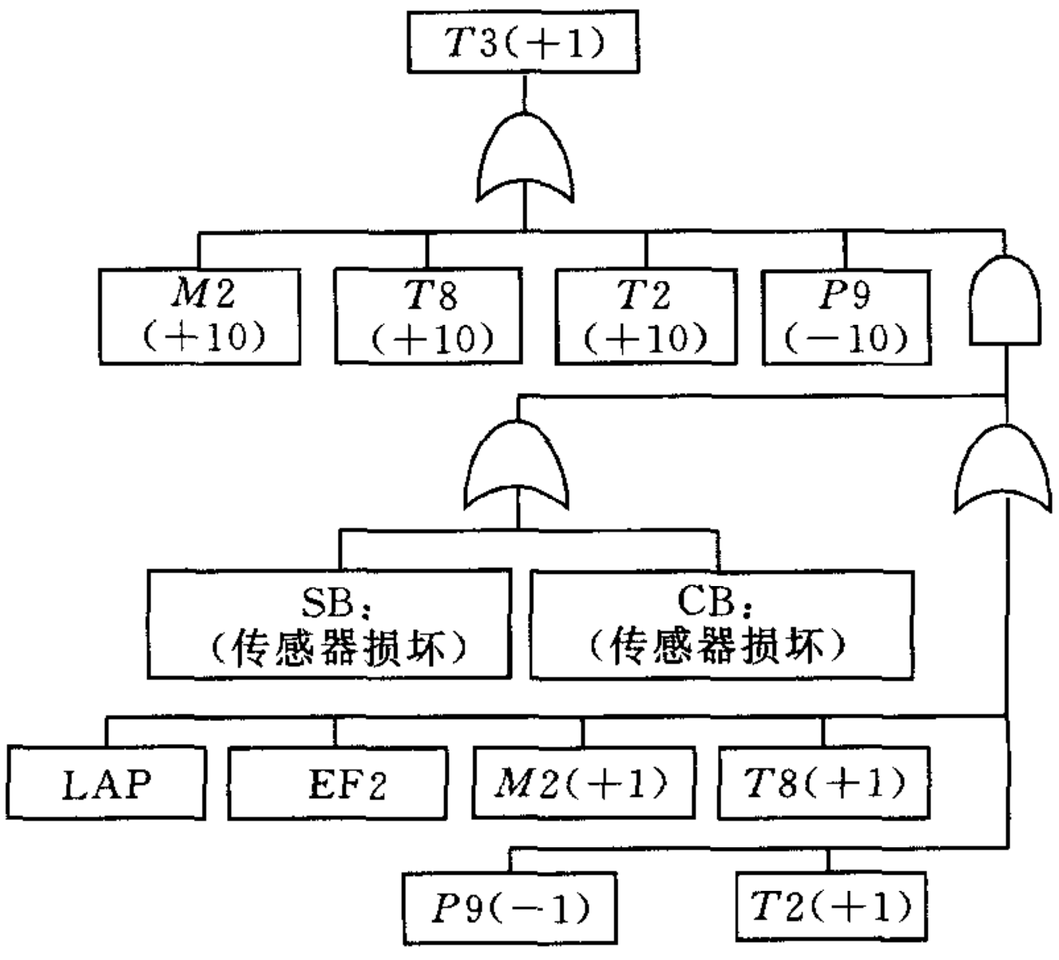

图 3　$T3$出现中等偏差时的故障树

Fig. 3　Fault tree for event $T3(+1)$

由上边典型案例的故障自动建树过程可以看出，本文提出的规范化形式描述及基于CSP的自动建树求解过程简洁有效，利于计算机自动处理，与系统的实际情况比较吻合.

References

1 Lu Ting-Xiao, Zheng Peng-Zhou. Reliability Analysis and Design. Beijing: National Defence Industry Press, 1995 (in Chinese)

2 Wen Xin, Zhang Hong-Yue, Zhou Lu. Fault Diagnosis and Fault-tolerant Control for Control System. Beijing: China Machine Press, 1998(in Chinese)

3 Zen Tian-Xiang. Testability and Fault Diagnostic Technology for Electronic Equipment. Beijing: Aviation Industry Press, 1996(in Chinese)

4 Carpignano A, Poucet A. Computer assisted fault tree construction: A review of methods and concerns. *Reliability Engineering and System Safety*, 1994, **44**(3): 265～278

5 Jian Zhi-Min, Hu Dong-Cheng, Tong Shi-Bai. A new methodology of automatic construction of fault trees for control systems. *Acta Automatica Sinica*, 1997, **23**(3): 314～318(in Chinese)

6 Andow P K. Difficulties in fault tree synthesis for process plant. *IEEE Transactions on Reliability*, 1980, **29**(1): 2～8

7 Bossche A. Computer-aided fault tree synthesis I——System modeling and casual trees. *Reliability Engineering and System Safety*, 1991, **32**(3): 217～241

8 Lapp S A, Powers G J. Computer-aided synthesis of falut-tree. *IEEE Transactions on Reliability*, 1977, **26**(4): 2～14

9 Tao Jun, Li Ying-Hong, Xin Yu-Feng. Research on automatic fault tree construction for control system. *Acta Automatica Sinica*, 1997, **23**(6): 822～826(in Chinese)

10 Andrews J D, Morgan J M. Application of the digraph method of fault tree construction to process plant. *Reliability Engineering and System Safety*, 1986, **14**(2): 85～106

11 Andrews J D, Brennan G. Application of the digraph method of fault tree construction to a complex control configuration. *Reliability Engineering and System Safety*, 1990, **28**(3): 357～384

12 Kumar V. Algorithms for constraint satisfaction problem: A survey. *AI Magazine*, 1992, **13**(1): 32～44

13 Qian Xue-Sen. On System Engineer. Changsha: Hunan Science & Technology Press, 1998(in Chinese)

14 He Xin-Gui. Theory and Techniques for Fuzzy Knowledge Processing(2nd Edition). Beijing: National Defence Industry Press, 1998(in Chinese)

钱彦岭 博士研究生. 主要研究兴趣为状态监控与故障诊断、复杂设备测试性设计等.

(**QIAN Yan-Ling** Ph. D. candidate. His research interests include state monitoring and fault diagnosis, design for testability for complex mechatronic systems.)

邱 静 博士，教授. 主要从事状态监控与故障诊断、动态系统测试与分析方面的科研和教学工作.

(**QIU Jing** Ph. D., professor. His research interests include state monitoring and fault diagnosis, test and analysis for dynamic system.)